BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

#2

Docket No. 1341.1076 (JDH)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	
	)	
Masahiro KOMURA, et al.	)	
	)	Group Art Unit: Unassigned
Serial No.: To be assigned	)	
	)	Examiner: Unassigned
Filed: December 20, 2000	)	

For: **A METHOD AND APPARATUS FOR MEDIATION OF SECURITY INFORMATION, AND A COMPUTER PRODUCT**

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Assistant Commissioner for Patents
Washington, D.C. 2023l

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-234555
Filed: August 2, 2000.

It is respectfully requested that the applicants be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,
STAAS & HALSEY LLP

By: _____
James D. Halsey, Jr.
Registration No. 22,729

Date: December 20, 2000
700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

PFJA-00051-US #2

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ８月 ２日

出 願 番 号
Application Number: 特願２０００－２３４５５５

出 願 人
Applicant (s): 富士通株式会社

２０００年１０月２７日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２０００－３０８９７７３

【書類名】　特許願

【整理番号】　0050561

【提出日】　平成12年 8月 2日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/60

【発明の名称】　セキュリティ情報仲介装置、セキュリティ情報仲介方法およびセキュリティ情報仲介プログラムを記録したコンピュータ読み取り可能な記録媒体

【請求項の数】　15

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小村　昌弘

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小谷　誠剛

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　鳥居　悟

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100089118

【弁理士】

【氏名又は名称】　酒井　宏明

【手数料の表示】

【予納台帳番号】　036711

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9717671

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セキュリティ情報仲介装置、セキュリティ情報仲介方法およびセキュリティ情報仲介プログラムを記録したコンピュータ読み取り可能な記録媒体

【特許請求の範囲】

【請求項１】　情報提供者の情報提供者端末から提供されたセキュリティ情報を登録する登録手段と、

前記セキュリティ情報の有用性を判断する情報受信者の情報受信者端末へ、前記登録手段により登録された前記セキュリティ情報を転送する第１の転送手段と、

当該セキュリティ情報の有用性を示す返答情報および当該セキュリティ情報の情報提供料の支払いに関する支払情報を前記情報受信者端末より受信する受信手段と、

前記返答情報および前記支払情報を前記情報提供者端末へ転送する第２の転送手段と、

を備えたことを特徴とするセキュリティ情報仲介装置。

【請求項２】　前記登録手段は、登録済みのセキュリティ情報を参照し、提供されたセキュリティ情報が新規である場合にのみ、当該セキュリティ情報を登録し、前記第１の転送手段は、提供されたセキュリティ情報が新規である場合にのみ、当該セキュリティ情報を前記情報受信者端末へ転送することを特徴とする請求項１に記載のセキュリティ情報仲介装置。

【請求項３】　前記情報受信者が所望するセキュリティ情報の分類情報を登録する分類情報登録手段と、前記情報提供端末から提供されたセキュリティ情報を分類する分類手段とを備え、前記第１の転送手段は、前記分類情報と前記分類手段の分類結果が一致する場合にのみ当該セキュリティ情報を前記情報受信者端末へ転送することを特徴とする請求項１または２に記載のセキュリティ情報仲介装置。

【請求項４】　前記受信手段は、当該セキュリティ情報の無効を示す無効情報を前記情報受信者端末より受信し、前記第２の転送手段は、前記無効情報を前

記情報提供者端末へ転送することを特徴とする請求項１～３のいずれか一つに記載のセキュリティ情報仲介装置。

【請求項５】　前記受信手段は、有用性が示されたセキュリティ情報の対策用の修正情報を受信し、前記第２の転送手段は、前記修正情報を前記情報提供者端末へ転送することを特徴とする請求項１～４のいずれか一つに記載のセキュリティ情報仲介装置。

【請求項６】　前記登録手段により登録された前記セキュリティ情報を公開する公開手段を備えたことを特徴とする請求項１～５のいずれか一つに記載のセキュリティ情報仲介装置。

【請求項７】　前記登録手段により登録されたセキュリティ情報および前記修正情報を公開する公開手段を備えたことを特徴とする請求項５に記載のセキュリティ情報仲介装置。

【請求項８】　情報提供者の情報提供者端末から提供されたセキュリティ情報を登録する登録工程と、

前記セキュリティ情報の有用性を判断する情報受信者の情報受信者端末へ、前記登録工程で登録された前記セキュリティ情報を転送する第１の転送工程と、

当該セキュリティ情報の有用性を示す返答情報および当該セキュリティ情報の情報提供料の支払いに関する支払情報を前記情報受信者端末より受信する受信工程と、

前記返答情報および前記支払情報を前記情報提供者端末へ転送する第２の転送工程と、

を含むことを特徴とするセキュリティ情報仲介方法。

【請求項９】　前記登録工程では、登録済みのセキュリティ情報を参照し、提供されたセキュリティ情報が新規である場合にのみ、当該セキュリティ情報を登録し、前記第１の転送工程では、提供されたセキュリティ情報が新規である場合にのみ、当該セキュリティ情報を前記情報受信者端末へ転送することを特徴とする請求項８に記載のセキュリティ情報仲介方法。

【請求項１０】　前記情報受信者が所望するセキュリティ情報の分類情報を登録する分類情報登録工程と、前記情報提供端末から提供されたセキュリティ情

報を分類する分類工程とを含み、前記第１の転送工程では、前記分類情報と前記分類工程の分類結果が一致する場合にのみ当該セキュリティ情報を前記情報受信者端末へ転送することを特徴とする請求項８または９に記載のセキュリティ情報仲介方法。

【請求項１１】　前記受信工程では、当該セキュリティ情報の無効を示す無効情報を前記情報受信者端末より受信し、前記第２の転送工程では、前記無効情報を前記情報提供者端末へ転送することを特徴とする請求項８～１０のいずれか一つに記載のセキュリティ情報仲介方法。

【請求項１２】　前記受信工程では、有用性が示されたセキュリティ情報の対策用の修正情報を受信し、前記第２の転送工程では、前記修正情報を前記情報提供者端末へ転送することを特徴とする請求項８～１１のいずれか一つに記載のセキュリティ情報仲介方法。

【請求項１３】　前記登録工程で登録された前記セキュリティ情報を公開する公開工程を含むことを特徴とする請求項８～１２のいずれか一つに記載のセキュリティ情報仲介方法。

【請求項１４】　前記登録工程で登録されたセキュリティ情報および前記修正情報を公開する公開工程を含むことを特徴とする請求項１２に記載のセキュリティ情報仲介方法。

【請求項１５】　前記請求項８～１４のいずれか一つに記載のセキュリティ情報仲介方法をコンピュータに実行させるためのセキュリティ情報仲介プログラムを記録したコンピュータ実行可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータプログラムの開発元（ベンダ）とユーザとの間で、セキュリティホールに関するセキュリティ情報を効率的に仲介させるセキュリティ情報仲介装置、セキュリティ情報仲介方法およびセキュリティ情報仲介プログラムを記録したコンピュータ読み取り可能な記録媒体に関するものである。

【０００２】

近時、コンピュータプログラムのセキュリティ情報に関する情報交換および情報公開は、ＣＥＲＴやその他のボランティア団体、民間企業により、インターネットを介して世界規模で行われている。ここでいうセキュリティ情報とは、コンピュータプログラムの設計上のミスやバグ等によってセキュリティ対策上問題となるセキュリティホールに関する情報をいう。

【０００３】

しかしながら、現状では、セキュリティホールを発見した善意者が、危険なクラッカーと間違われたり、コンピュータプログラム開発会社とのトラブルに巻き込まれる等の問題が発生していることから、セキュリティ情報の交換および公開をオープンに誰もが行うことができる環境が整っているとは言い難い。これは、インターネットをはじめとするオープンシステムの流れに逆行し、人類共有の資産であるコンピュータプログラムの発展を阻害するものである。このような背景より、かかる問題を効果的に解決するための手段、方法が切望されている。

【０００４】

【従来の技術】

コンピュータプログラムの開発元では、テスト段階で設計ミスやバグ等のセキュリティホールを徹底的に洗い出し、対策済みのコンピュータプログラムをユーザに提供している。しかしながら、現実的には、テスト段階でセキュリティホールの全てを発見することが極めて困難であるため、ユーザが当該コンピュータプログラムを利用してはじめて、開発元で発見できなかったセキュリティホールが発見される場合が多い。

【０００５】

ここで、セキュリティホールを発見したユーザは、セキュリティホールの詳細情報をセキュリティ情報として、直接、開発元に提供したり、インターネット上のセキュリティ情報サイトにセキュリティ情報を投稿する等の対応を採る場合がある。この場合、開発元では、提供されたセキュリティ情報が有用であると判断すると、修正用のパッチプログラムや当該セキュリティ情報をユーザに提供する等の対応をとる。

【０００６】

【発明が解決しようとする課題】

ところで、前述したように、従来では、直接やインターネット上のセキュリティ情報サイトを介して、ユーザから開発元へセキュリティ情報を提供する環境がある。しかしながら、従来では、善意でセキュリティ情報を提供したユーザが、危険なクラッカと酷評されたり、セキュリティホールの存在を公開したくない開発元とのトラブルに巻き込まれたりする場合が多い。

【０００７】

従って、従来では、有用なセキュリティ情報を有するユーザが、上述した酷評やトラブルを避け、当該セキュリティ情報の提供を躊躇してしまう環境があることも否めない。このような環境は、コンピュータプログラムの質向上を妨げ、開発元およびユーザにとって利益とならない。

【０００８】

一方、開発元では、インターネット上に分散されたセキュリティ情報を効率良く収集することが困難であり、しかも質にバラツキがあるセキュリティ情報の中から有用なものを選別しなければならないため、労力やコストも看過できない状況にある。ここで、分散されたセキュリティ情報を分類する動きがあるが、際だった成果が見られない。結局、開発元は、独自に大量のセキュリティ情報を収集し、この中から有用なものを選別するという従来の手法を踏襲せざるを得ないのである。

【０００９】

本発明は、上記に鑑みてなされたもので、ユーザにとってセキュリティ情報を提供し易い環境を整備することができ、しかも開発元にとって低コストで有用なセキュリティ情報を収集することができるセキュリティ情報仲介装置、セキュリティ情報仲介方法およびセキュリティ情報仲介プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【００１０】

【課題を解決するための手段】

上記目的を達成するために、本発明は、情報提供者の情報提供者端末から提供されたセキュリティ情報を登録する登録手段と、前記セキュリティ情報の有用性

を判断する情報受信者の情報受信者端末へ、前記登録手段により登録された前記セキュリティ情報を転送する第１の転送手段と、当該セキュリティ情報の有用性を示す返答情報および当該セキュリティ情報の情報提供料の支払いに関する支払情報を前記情報受信者端末より受信する受信手段と、前記返答情報および前記支払情報を前記情報提供者端末へ転送する第２の転送手段とを備えたことを特徴とする。

【００１１】

この発明によれば、情報提供者（ユーザ）よりセキュリティ情報が提供されると、登録手段によりセキュリティ情報が登録される。これにより、第１の転送手段により、上記セキュリティ情報が情報受信者端末（例えば、コンピュータプログラムの開発元の端末）へ転送され、情報受信者によりセキュリティ情報の有用性が判断される。ここで、セキュリティ情報が有用であると判断されると、情報受信者端末からは、返答情報および支払情報が送信される。

【００１２】

そして、上記返答情報および支払情報が受信手段に受信されると、第２の転送手段は、返答情報および支払情報を情報提供者端末へ転送する。これにより、情報提供者は、自身が提供したセキュリティ情報が有用であることを認識するとともに、セキュリティ情報の提供に対する支払いがあることを認識する。

【００１３】

このように、この発明によれば、情報提供者からのセキュリティ情報をダイレクトに情報受信者側に提供し、しかも有用なセキュリティ情報を提供した者に対して支払いを行うようにしたので、情報提供者（ユーザ）にとってセキュリティ情報を提供し易い環境を整備し、情報受信者（例えば、開発元）にとって低コストで有用なセキュリティ情報を収集することができる。

【００１４】

また、本発明は、情報提供者の情報提供者端末から提供されたセキュリティ情報を登録する登録工程と、前記セキュリティ情報の有用性を判断する情報受信者の情報受信者端末へ、前記登録工程で登録された前記セキュリティ情報を転送する第１の転送工程と、当該セキュリティ情報の有用性を示す返答情報および当該

セキュリティ情報の情報提供料の支払いに関する支払情報を前記情報受信者端末より受信する受信工程と、前記返答情報および前記支払情報を前記情報提供者端末へ転送する第２の転送工程とを含むことを特徴とする。

【００１５】

この発明によれば、情報提供者（ユーザ）よりセキュリティ情報が提供されると、登録工程でセキュリティ情報が登録される。これにより、第１の転送工程で上記セキュリティ情報が情報受信者端末（例えば、コンピュータプログラムの開発元の端末）へ転送され、情報受信者によりセキュリティ情報の有用性が判断される。ここで、セキュリティ情報が有用であると判断されると、情報受信者端末からは、返答情報および支払情報が送信される。

【００１６】

そして、受信工程で上記返答情報および支払情報が受信されると、第２の転送工程では、返答情報および支払情報が情報提供者端末へ転送される。これにより、情報提供者は、自身が提供したセキュリティ情報が有用であることを認識するとともに、セキュリティ情報の提供に対する支払いがあることを認識する。

【００１７】

このように、この発明によれば、情報提供者からのセキュリティ情報をダイレクトに情報受信者側に提供し、しかも有用なセキュリティ情報を提供した者に対して支払いを行うようにしたので、情報提供者（ユーザ）にとってセキュリティ情報を提供し易い環境を整備し、情報受信者（例えば、開発元）にとって低コストで有用なセキュリティ情報を収集することができる。

【００１８】

【発明の実施の形態】

以下、図面を参照して本発明にかかるセキュリティ情報仲介装置、セキュリティ情報仲介方法およびセキュリティ情報仲介プログラムを記録したコンピュータ読み取り可能な記録媒体の実施の形態１～４について詳細に説明する。

【００１９】

（実施の形態１）

図１は、本発明にかかる実施の形態１の構成を示すブロック図である。この図

において、ユーザクライアント１１は、ユーザ１０により操作されるコンピュータ端末であり、ネットワーク１２を介してセキュリティ情報仲介装置２０にアクセス可能とされている。ユーザ１０は、後述する開発元３１Ａや開発元３１Ｂ、その他の開発元により開発された各種コンピュータプログラムを利用する者である。また、ユーザ１０は、コンピュータプログラムのバグ等のセキュリティホールを発見し、これをセキュリティ情報として提供することができる知識を有する者である。

【００２０】

また、ユーザクライアント１１は、ネットワーク１２を介してセキュリティ情報仲介装置２０にセキュリティ情報４０を登録する機能と、セキュリティ情報４０が有用である場合にセキュリティ情報仲介装置２０から返答情報４１Ａおよび支払情報４２を受信する機能とを備えている。このセキュリティ情報４０は、ユーザ１０がコンピュータプログラムにセキュリティホールを発見した場合に、当該コンピュータプログラムの開発元へ提供される情報である。

【００２１】

具体的には、図２（ａ）に示したセキュリティ情報４０は、「登録者」（ユーザ１０）および「セキュリティ情報の内容」（ソフトウェアＸのバグ問題）から構成されている。「登録者」は、当該セキュリティ情報を登録した者を表す情報であり、「セキュリティ情報の内容」は、当該セキュリティ情報の具体的内容を表す情報である。

【００２２】

返答情報４１Ａは、セキュリティ情報４０が有効であると開発元に判断された場合に、当該開発元からユーザ１０へ返答される情報である。具体的には、図２（ｂ）に示した返答情報４１Ａは、「返答者」（開発元３１Ａ）、「判定結果」（有効）、「登録者」（ユーザ１０）および「セキュリティ情報の内容」（ソフトウェアＸのバグ問題）から構成されている。

【００２３】

「返答者」は、セキュリティ情報仲介装置２０に登録されたセキュリティ情報に対して返答した開発元を表す情報である。「判定結果」は、当該セキュリティ

情報が有効であるか否かの結果を表す情報である。「登録者」は、当該セキュリティ情報を登録した者を表す情報であり、「セキュリティ情報の内容」は、当該セキュリティ情報の具体的内容を表す情報である。

【００２４】

支払情報４２は、開発元３１Ａ側でセキュリティ情報４０が有効であると判定された場合に、セキュリティ情報４０を提供した代償として、開発元３１Ａからユーザ１０へ支払われる金額や、支払い方法等に関する情報である。具体的には、図２（ｄ）に示した支払情報４２は、「支払金額」（１００００円）、「支払先」（ユーザ１０）、「支払者」（開発元３１Ａ）および「支払方法」（電子決済）から構成されている。

【００２５】

「支払金額」は、セキュリティ情報４０を提供した代償として開発元３１Ａからユーザ１０へ支払われる金額を表す情報である。「支払先」は、上記金額の支払い先を表す情報である。「支払者」は、上記金額を支払う者を表す情報である。「支払方法」は、上記金額を支払者に支払う方法を表す情報である。なお、実施の形態１では、「支払方法」として電子決済を一例としているが、金融機関口座への振り込み等、他の支払い方法を用いてもよい。

【００２６】

セキュリティ情報仲介装置２０は、ユーザ１０と開発元３１Ａおよび３１Ｂとの間においてセキュリティ情報を仲介するサーバであり、ネットワーク１２とネットワーク３２との間に介挿されている。このセキュリティ情報仲介装置２０には、ユーザクライアント１１、開発元クライアント３０Ａおよび３０Ｂがアクセスする。

【００２７】

セキュリティ情報仲介装置２０において、セキュリティ情報登録部２１は、ユーザクライアント１１からのセキュリティ情報４０をセキュリティ情報データベース２２に登録する機能を備えている。なお、実際には、ネットワーク１２には、ユーザクライアント１１以外に多数のユーザクライアントが接続されている。従って、セキュリティ情報登録部２１は、他のユーザクライアントからのセキュ

リティ情報をセキュリティ情報データベース２２に登録する機能も備えている。

【００２８】

転送部２３は、セキュリティ情報登録部２１により登録されたセキュリティ情報を、ネットワーク３２を介して開発元クライアント３０Ａおよび３０Ｂに転送する機能を備えている。ネットワーク３２は、セキュリティ情報仲介装置２０と開発元クライアント３０Ａおよび３０Ｂとを接続するものである。開発元クライアント３０Ａは、コンピュータプログラムのベンダである開発元３１Ａ側に設置されたコンピュータ端末である。開発元クライアント３０Ｂは、コンピュータプログラムのベンダである開発元３１Ｂ側に設置されたコンピュータ端末である。

【００２９】

開発元クライアント３０Ａは、転送部２３からのセキュリティ情報４０を受信し、上述した返答情報４１Ａ（図２（ｂ）参照）および支払情報４２（図２（ｄ）参照）をセキュリティ情報仲介装置２０へ送信する。同様にして、開発元クライアント３０Ｂは、転送部２３からのセキュリティ情報４０を受信し、返答情報４１Ｂをセキュリティ情報仲介装置２０へ送信する。

【００３０】

同図に示した例では、開発元クライアント３０Ｂからは、支払情報が送信されない。これは、セキュリティ情報４０が開発元３１Ｂにとって無効であり、代償としての支払いが発生しないからである。つまり、返答情報４１Ａ（図２（ｂ）参照）の「判定結果」が有効であるのに対して、返答情報４１Ｂ（図２（ｃ）参照）の「判定結果」は、無効である。この場合、返答情報４１Ｂの「返答者」は、開発元３１Ｂとされている。

【００３１】

セキュリティ情報仲介装置２０において、返答情報登録部２４は、開発元クライアント３０Ａおよび開発元クライアント３０Ｂからネットワーク３２を介して送信される返答情報４１Ａ、支払情報４２および返答情報４１Ｂを返答情報データベース２５に登録する機能を備えている。転送部２６は、返答情報登録部２４に登録された返答情報のうち「判定結果」が有効とされた返答情報（同図では返答情報４１Ａ）と、該返答情報に対応する支払情報（同図では支払情報４２）と

を、ネットワーク１２を介して当該ユーザクライアント（同図ではユーザクライアント１１）に転送する機能を備えている。

【００３２】

つぎに、実施の形態１の動作について、図３に示したフローチャートを参照しつつ説明する。同図に示したステップＳＡ１では、セキュリティ情報登録部２１は、ユーザクライアント１１からセキュリティ情報を受信したか否かを判断し、この場合、判断結果を「Ｎｏ」として同判断を繰り返す。ここで、ソフトウェアＸのバグ（セキュリティホール）を発見したユーザ１０は、図２（ａ）に示したセキュリティ情報４０をユーザクライアント１１により作成する。つぎに、ユーザ１０の操作により、ユーザクライアント１１からセキュリティ情報仲介装置２０へセキュリティ情報４０が送信される。

【００３３】

そして、上記セキュリティ情報４０を受信すると、セキュリティ情報登録部２１は、ステップＳＡ１の判断結果を「Ｙｅｓ」とする。ステップＳＡ２では、セキュリティ情報登録部２１は、セキュリティ情報４０をセキュリティ情報データベース２２に登録する。ステップＳＡ３では、セキュリティ情報登録部２１は、セキュリティ情報４０を転送部２３へ渡す。これにより、転送部２３は、セキュリティ情報４０を開発元クライアント３０Ａおよび３０Ｂに並列的に転送する。ステップＳＡ４では、返答情報登録部２４は、返答情報を受信したか否かを判断し、この場合、判断結果を「Ｎｏ」として同判断を繰り返す。

【００３４】

そして、開発元クライアント３０Ａおよび３０Ｂによりセキュリティ情報４０がそれぞれ受信されると、開発元３１Ａおよび３１Ｂは、セキュリティ情報４０が有効な情報であるか否かをそれぞれ判断する。ここで「有効」とは、セキュリティ情報４０が、当該ソフトウェアＸのバージョンアップに貢献し、かつ提供の代償としてユーザ１０に対して所定の金額を支払うことが妥当であると判断された状態をいう。

【００３５】

この場合、開発元３１Ａでは、セキュリティ情報４０が有効であると判断され

たものとする。開発元３１Ａでは、開発元クライアント３０Ａを用いて、返答情報４１Ａ（図２（ｂ）参照）および支払情報４２（図２（ｄ）参照）を作成した後、これらをセキュリティ情報仲介装置２０宛に送信する。これらの返答情報４１Ａおよび支払情報４２は、ネットワーク３２を介してセキュリティ情報仲介装置２０の返答情報登録部２４に受信される。

【００３６】

これにより、返答情報登録部２４は、ステップＳＡ４の判断結果を「Ｙｅｓ」とする。ステップＳＡ５では、返答情報登録部２４は、図２（ｂ）に示した返答情報４１Ａの「判定結果」が有効であるか否かを判断し、この場合、判断結果を「Ｙｅｓ」とする。ステップＳＡ６では、返答情報登録部２４は、受信した返答情報４１Ａに対応する支払情報を受信したか否かを判断し、この場合、判断結果を「Ｙｅｓ」とする。なお、ステップＳＡ６の判断結果が「Ｎｏ」である場合、返答情報登録部２４は、同判断を繰り返す。

【００３７】

ステップＳＡ７では、返答情報登録部２４は、返答情報４１Ａおよび支払情報４２を返答情報データベース２５に登録する。ステップＳＡ８では、返答情報登録部２４は、返答情報４１Ａおよび支払情報４２を転送部２６へ渡す。これにより、転送部２６は、返答情報４１Ａおよび支払情報４２をネットワーク１２を介してユーザクライアント１１へ転送する。

【００３８】

これらの返答情報４１Ａおよび支払情報４２がユーザクライアント１１に受信されると、ユーザクライアント１１は、返答情報４１Ａおよび支払情報４２をユーザ１０に報知する。これにより、ユーザ１０は、自身が提供したセキュリティ情報４０が有用であったことを認識するとともに、電子決済により開発元３１Ａから１００００円が支払われることを認識する。

【００３９】

一方、開発元３１Ｂでは、セキュリティ情報４０が無効な情報であると判断したものとする。ここでいう「無効」とは、当該ソフトウェアＸが開発元３１Ｂと無関係であって、かつ提供の代償としてユーザに対して所定の金額を支払う必要

がない状態をいう。この場合、開発元３１Ｂでは、開発元クライアント３０Ｂを用いて、無効である旨の返答情報４１Ｂ（図２（ｃ）参照）を作成した後、これをセキュリティ情報仲介装置２０宛に送信する。この返答情報４１Ｂは、ネットワーク３２を介してセキュリティ情報仲介装置２０の返答情報登録部２４に受信される。

【００４０】

これにより、返答情報登録部２４は、ステップＳＡ４の判断結果を「Ｙｅｓ」とする。ステップＳＡ５では、返答情報登録部２４は、図２（ｃ）に示した返答情報４１Ｂの「判定結果」が有効であるか否かを判断し、この場合、判断結果を「Ｎｏ」とする。ステップＳＡ９では、返答情報４１Ｂを返答情報データベース２５に登録する。

【００４１】

以上説明したように、実施の形態１によれば、ユーザ１０からのセキュリティ情報４０をダイレクトに開発元３１Ａおよび開発元３１Ｂに提供し、しかも有用なセキュリティ情報を提供した者に対して支払いを行うようにしたので、ユーザ１０にとってセキュリティ情報を提供し易い環境を整備し、開発元３１Ａおよび開発元３１Ｂにとって低コストで有用なセキュリティ情報を収集することができる。

【００４２】

（実施の形態２）

図４は、本発明にかかる実施の形態２の構成を示すブロック図である。この図において、ユーザクライアント１０１Ａは、ユーザ１００Ａにより操作されるコンピュータ端末であり、ネットワーク１０２を介してセキュリティ情報仲介装置２００にアクセス可能とされている。ユーザ１００Ａは、後述する開発元３０１、その他の開発元により開発された各種コンピュータプログラムを利用する者である。また、ユーザ１００Ａは、コンピュータプログラムのバグ等のセキュリティホールを発見し、これをセキュリティ情報として提供することができる知識を有するものである。

【００４３】

また、ユーザクライアント１０１Ａは、ユーザクライアント１１（図１参照）と同様にして、ネットワーク１０２を介してセキュリティ情報仲介装置２００にセキュリティ情報４００Ａを登録する機能と、セキュリティ情報仲介装置２００からの情報（同図では、返答情報４０１Ａおよび支払情報４０２）を受信する機能とを備えている。

【００４４】

上記セキュリティ情報４００Ａは、ユーザ１００Ａがコンピュータプログラムにセキュリティホールを発見した場合に、当該コンピュータプログラムの開発元へ提供される情報であり、セキュリティ情報４０（図２（ａ）参照）と同一の構成とされている。具体的には、図５（ａ）に示したセキュリティ情報４００Ａは、「登録者」（ユーザ１００Ａ）および「セキュリティ情報の内容」（ソフトウェアＸのバグ問題ＱＡ）から構成されている。

【００４５】

返答情報４０１Ａは、返答情報４１Ａ（図２（ｂ）参照）と同様にして、セキュリティ情報４００Ａが有効であると開発元に判断された場合に、当該開発元からユーザ１００Ａへ返答される情報である。具体的には、図５（ｃ）に示した返答情報４０１Ａは、「返答者」（開発元３０１）、「判定結果」（有効）、「登録者」（ユーザ１００Ａ）および「セキュリティ情報の内容」（ソフトウェアＸのバグ問題ＱＡ）から構成されている。

【００４６】

支払情報４０２は、支払情報４２（図２（ｄ）参照）と同様にして、開発元３０１側でセキュリティ情報４００Ａが有効であると判断された場合に、セキュリティ情報４００Ａを提供した代償として、開発元３０１からユーザ１００Ａへ支払われる金額や、支払い方法等に関する情報である。具体的には、図５（ｅ）に示した支払情報４０２は、「支払金額」（１００００円）、「支払先」（ユーザ１００Ａ）、「支払者」（開発元３０１）および「支払方法」（電子決済）から構成されている。

【００４７】

一方、ユーザクライアント１０１Ｂは、ユーザ１００Ｂにより操作されるコン

ピュータ端末であり、ネットワーク１０２を介してセキュリティ情報仲介装置２００にアクセス可能とされている。ユーザ１００Ｂは、ユーザ１００Ａと同様にして、開発元３０１、その他の開発元により開発された各種コンピュータプログラムを利用する者である。また、ユーザ１００Ｂは、コンピュータプログラムのバグ等のセキュリティホールを発見し、これをセキュリティ情報として提供することができる知識を有するものである。

【００４８】

また、ユーザクライアント１０１Ｂは、ユーザクライアント１０１Ａと同様にして、ネットワーク１０２を介してセキュリティ情報仲介装置２００にセキュリティ情報４００Ｂを登録する機能と、セキュリティ情報仲介装置２００からの情報（同図では返答情報４０１Ｂ）を受信する機能とを備えている。

【００４９】

このセキュリティ情報４００Ｂは、ユーザ１００Ｂがコンピュータプログラムにセキュリティホールを発見した場合に、当該コンピュータプログラムの開発元へ提供される情報であり、セキュリティ情報４０（図２（ａ）参照）と同一の構成とされている。具体的には、図５（ｂ）に示したセキュリティ情報４００Ｂは、「登録者」（ユーザ１００Ｂ）および「セキュリティ情報の内容」（ソフトウェアＸのバグ問題ＱＢ）から構成されている。

【００５０】

返答情報４０１Ｂは、セキュリティ情報４００Ｂが無効であると開発元に判断された場合に、当該開発元からユーザ１００Ｂへ返答される情報である。具体的には、図５（ｄ）に示した返答情報４０１Ｂは、「返答者」（開発元３０１）、「判定結果」（無効）、「登録者」（ユーザ１００Ｂ）および「セキュリティ情報の内容」（ソフトウェアＸのバグ問題ＱＢ）から構成されている。

【００５１】

セキュリティ情報仲介装置２００は、ユーザ１００Ａおよび１００Ｂと開発元３０１との間においてセキュリティ情報を仲介するサーバであり、ネットワーク１０２とネットワーク３０２との間に介挿されている。このセキュリティ情報仲介装置２００には、ユーザクライアント１０１Ａ、１０１Ｂ、開発元クライアン

ト３００がアクセスする。

【００５２】

セキュリティ情報仲介装置２００において、受信部２０１は、ユーザクライアント１０１Ａおよび１０１Ｂからのセキュリティ情報４００Ａおよび４００Ｂを受信する機能を備えている。情報管理部２０２は、受信部２０１に受信されたセキュリティ情報４００Ａおよび４００Ｂや、後述する受信部２０６に受信された返答情報４０１Ａ、４０１Ｂおよび支払情報４０２を管理する機能を備えている。この情報管理部２０２の機能については、後述する。

【００５３】

転送部２０５は、情報管理部２０２により登録されたセキュリティ情報を、ネットワーク３０２を介して開発元クライアント３００に転送する機能を備えている。ネットワーク３０２は、セキュリティ情報仲介装置２００と開発元クライアント３００とを接続するものである。開発元クライアント３００は、コンピュータプログラムのベンダである開発元３０１側に設置されたコンピュータ端末である。

【００５４】

開発元クライアント３００は、転送部２０５からのセキュリティ情報４００Ａおよび４００Ｂを受信し、上述した返答情報４０１Ａ（図５（ｃ）参照）、返答情報４０１Ｂ（図５（ｄ）参照）および支払情報４０２（図５（ｅ）参照）をセキュリティ情報仲介装置２００へ送信する。

【００５５】

同図に示した例では、開発元クライアント３００からは、セキュリティ情報４００Ｂに対応する支払情報が送信されない。これは、セキュリティ情報４００Ｂが開発元３０１にとって無効であり、代償としての支払いが発生しないからである。つまり、返答情報４０１Ａ（図５（ｃ）参照）の「判定結果」が有効であるのに対して、返答情報４０１Ｂ（図５（ｄ）参照）の「判定結果」は、無効である。この場合、返答情報４０１Ａおよび４０１Ｂのそれぞれの「返答者」は、共に開発元３０１とされている。

【００５６】

セキュリティ情報仲介装置２００において、受信部２０６は、開発元クライアント３００からネットワーク３０２を介して送信される返答情報、支払情報（同図では、返答情報４０１Ａ、４０１Ｂ、支払情報４０２）を受信する機能を備えている。情報管理部２０２は、受信部２０１に受信されたセキュリティ情報（同図では、セキュリティ情報４００Ａおよび４００Ｂ）を図６（ａ）に示したセキュリティ情報データベース２０３に登録する機能を備えている。

【００５７】

このセキュリティ情報データベース２０３は、セキュリティ情報に対して登録順に付与される「登録番号」、「登録日時」、「登録者」および「セキュリティ情報の内容」から構成されている。同図において、「登録番号」＝「３」のレコードは、セキュリティ情報４００Ａ（図５（ａ）参照）に対応しており、「登録番号」＝「４」のレコードは、セキュリティ情報４００Ｂ（図５（ｂ）参照）に対応している。

【００５８】

また、情報管理部２０２は、受信部２０６に受信された返答情報（同図では、返答情報４０１Ａおよび４０１Ｂ）を図６（ｂ）に示した返答情報データベース２０４に登録する機能を備えている。この返答情報データベース２０４は、返答情報に対して登録順に付与される「返答番号」、「返答日時」、「登録番号」（図６（ａ）参照）、「返答者」および「判定結果」から構成されている。同図において、「返答番号」＝「３」のレコードは、返答情報４０１Ａ（図５（ｃ）参照）に対応しており、「返答番号」＝「４」のレコードは、返答情報４０１Ｂ（図５（ｄ）参照）に対応している。

【００５９】

さらに、情報管理部２０２は、「判定結果」が「有効」または「無効」とされた返答情報（同図では返答情報４０１Ａおよび返答情報４０１Ｂ）と、支払情報（同図では支払情報４０２）とを転送部２０７へ渡す。転送部２０７は、情報管理部２０２からの返答情報、支払情報を当該ユーザクライアントへネットワーク１０２を介して転送する機能を備えている。

【００６０】

つぎに、実施の形態２の動作について、図７に示したフローチャートを参照しつつ説明する。同図に示したステップＳＢ１では、情報管理部２０２は、受信部２０１によりセキュリティ情報が受信されたか否かを判断し、この場合、判断結果を「Ｎｏ」として同判断を繰り返す。

【００６１】

ここで、ソフトウェアＸのバグ（セキュリティホール）を発見したユーザ１００Ａは、図５（ａ）に示したセキュリティ情報４００Ａをユーザクライアント１０１Ａにより作成する。つぎに、ユーザ１００Ａの操作により、ユーザクライアント１０１Ａからセキュリティ情報仲介装置２００へセキュリティ情報４００Ａが送信される。

【００６２】

そして、上記セキュリティ情報４００Ａが受信部２０１に受信されると、情報管理部２０２は、ステップＳＢ１の判断結果を「Ｙｅｓ」とする。ステップＳＢ２では、情報管理部２０２は、セキュリティ情報４００Ａの「登録者」および「セキュリティ情報の内容」をキーとして、図６（ａ）に示したセキュリティ情報データベース２０３を検索する。この場合、セキュリティ情報データベース２０３には、「登録番号」＝１および２のレコードのみが存在しているものとする。

【００６３】

ステップＳＢ３では、情報管理部２０２は、検索ヒットしたか否か、すなわち、セキュリティ情報４００Ａと同一の内容がセキュリティ情報データベース２０３に登録されているか否かを判断し、この判断結果が「Ｙｅｓ」である場合、ステップＳＢ１１では、情報管理部２０２は、登録拒絶をする。この場合、情報管理部２０２は、ステップＳＢ３の判断結果を「Ｎｏ」とする。

【００６４】

ステップＳＢ４では、情報管理部２０２は、セキュリティ情報４００Ａをセキュリティ情報データベース２０３（図６（ａ）参照）に登録する。これにより、セキュリティ情報データベース２０３には、「登録番号」＝３のレコード（セキュリティ情報４００Ａに対応）が追加される。

【００６５】

ステップＳＢ５では、情報管理部２０２は、上記セキュリティ情報４００Ａを転送部２０５へ渡す。これにより、転送部２０５は、セキュリティ情報４００Ａをネットワーク３０２を介して開発元クライアント３００に転送する。ステップＳＢ６では、情報管理部２０２は、受信部２０６により返答情報が受信されたか否かを判断し、この場合、判断結果を「Ｎｏ」として同判断を繰り返す。

【００６６】

そして、開発元クライアント３００によりセキュリティ情報４００Ａが受信されると、開発元３０１は、セキュリティ情報４００Ａが有効な情報であるか否かを判断する。この場合、開発元３０１では、セキュリティ情報４００Ａが有効であると判断されたものとする。開発元３０１では、開発元クライアント３００を用いて、返答情報４０１Ａ（図５（ｃ）参照）および支払情報４０２（図５（ｅ）参照）を作成した後、これらをセキュリティ情報仲介装置２００宛に送信する。これらの返答情報４０１Ａおよび支払情報４０２は、ネットワーク３０２を介してセキュリティ情報仲介装置２００の受信部２０６に受信される。

【００６７】

これにより、情報管理部２０２は、ステップＳＢ６の判断結果を「Ｙｅｓ」とする。ステップＳＢ７では、情報管理部２０２は、返答情報４０１Ａを返答情報データベース２０４（図６（ｂ）参照）に登録する。これにより、返答情報データベース２０４には、「返答番号」＝３のレコード（返答情報４０１Ａに対応）が追加される。

【００６８】

ステップＳＢ８では、情報管理部２０２は、図５（ｃ）に示した返答情報４０１Ａの「判定結果」が有効であるか否かを判断し、この場合、判断結果を「Ｙｅｓ」とする。ステップＳＢ９では、情報管理部２０２は、返答情報４０１Ａに対応する支払情報４０２が受信部２０６に受信されたか否かを判断し、この場合、判断結果を「Ｙｅｓ」とする。なお、ステップＳＢ９の判断結果が「Ｎｏ」である場合、情報管理部２０２は、同判断を繰り返す。

【００６９】

ステップＳＢ１０では、情報管理部２０２は、返答情報４０１Ａおよび支払情

報４０２を転送部２０７へ渡す。これにより、転送部２０７は、返答情報４０１Ａおよび支払情報４０２をネットワーク１０２を介してユーザクライアント１０１Ａへ転送する。

【００７０】

これらの返答情報４０１Ａおよび支払情報４０２がユーザクライアント１０１Ａに受信されると、ユーザクライアント１０１Ａは、返答情報４０１Ａおよび支払情報４０２をユーザ１００Ａに報知する。これにより、ユーザ１００Ａは、自身が提供したセキュリティ情報４００Ａが有用であったことを認識するとともに、電子決済により開発元３０１から１００００円が支払われることを認識する。

【００７１】

一方、ソフトウェアＸのバグ（セキュリティホール）を発見したユーザ１００Ｂは、図５（ｂ）に示したセキュリティ情報４００Ｂをユーザクライアント１０１Ｂにより作成する。つぎに、ユーザ１００Ｂの操作により、ユーザクライアント１０１Ｂからセキュリティ情報仲介装置２００へセキュリティ情報４００Ｂが送信される。

【００７２】

そして、上記セキュリティ情報４００Ｂが受信部２０１に受信されると、情報管理部２０２は、ステップＳＢ１の判断結果を「Ｙｅｓ」とする。ステップＳＢ２では、情報管理部２０２は、セキュリティ情報４００Ｂの「登録者」および「セキュリティ情報の内容」をキーとして、セキュリティ情報データベース２０３を検索する。この場合、セキュリティ情報データベース２０３には、「登録番号」＝１～３のレコードのみが存在しているものとする。

【００７３】

ステップＳＢ３では、情報管理部２０２は、検索ヒットしたか否かを判断し、この場合、判断結果を「Ｎｏ」とする。ステップＳＢ４では、情報管理部２０２は、セキュリティ情報４００Ｂをセキュリティ情報データベース２０３（図６（ａ）参照）に登録する。これにより、セキュリティ情報データベース２０３には、「登録番号」＝４のレコード（セキュリティ情報４００Ｂに対応）が追加される。

【００７４】

ステップＳＢ５では、情報管理部２０２は、上記セキュリティ情報４００Ｂを転送部２０５へ渡す。これにより、転送部２０５は、セキュリティ情報４００Ｂをネットワーク３０２を介して開発元クライアント３００に転送する。ステップＳＢ６では、情報管理部２０２は、受信部２０６により返答情報が受信されたか否かを判断し、この場合、判断結果を「Ｎｏ」として同判断を繰り返す。

【００７５】

そして、開発元クライアント３００によりセキュリティ情報４００Ｂが受信されると、開発元３０１は、セキュリティ情報４００Ｂが有効な情報であるか否かを判断する。この場合、開発元３０１では、セキュリティ情報４００Ｂが無効であると判断されたものとする。開発元３０１では、開発元クライアント３００を用いて、拒絶メッセージとしての返答情報４０１Ｂ（図５（ｄ）参照）を作成した後、これをセキュリティ情報仲介装置２００宛に送信する。

【００７６】

そして、返答情報４０１Ｂは、ネットワーク３０２を介してセキュリティ情報仲介装置２００の受信部２０６に受信される。これにより、情報管理部２０２は、ステップＳＢ６の判断結果を「Ｙｅｓ」とする。ステップＳＢ７では、情報管理部２０２は、返答情報４０１Ｂを返答情報データベース２０４（図６（ｂ）参照）に登録する。これにより、返答情報データベース２０４には、「返答番号」＝４のレコード（返答情報４０１Ｂに対応）が追加される。

【００７７】

ステップＳＢ８では、情報管理部２０２は、図５（ｄ）に示した返答情報４０１Ｂの「判定結果」が有効であるか否かを判断し、この場合、判断結果を「Ｎｏ」とする。ステップＳＢ１２では、情報管理部２０２は、拒絶メッセージとしての返答情報４０１Ｂを転送部２０７へ渡す。これにより、転送部２０７は、返答情報４０１Ｂをネットワーク１０２を介してユーザクライアント１０１Ｂへ転送する。この返答情報４０１Ｂがユーザクライアント１０１Ｂに受信されると、ユーザクライアント１０１Ｂは、返答情報４０１Ｂをユーザ１００Ｂに報知する。これにより、ユーザ１００Ｂは、自身が提供したセキュリティ情報４００Ｂが無

効であったことを認識する。

【００７８】

以上説明したように、実施の形態２によれば、ユーザ１００Ｂから提供されたセキュリティ情報４００Ｂの無効を示す返答情報４０１Ｂをユーザクライアント１０１Ｂへ転送するようにしたので、提供したセキュリティ情報の使われ方（有用または無効）に関心を持つユーザに対するサービスを向上させることができる。

【００７９】

また、実施の形態２によれば、ユーザ（ユーザ１００Ａ、１００Ｂ）より提供されたセキュリティ情報（セキュリティ情報４００Ａ、４００Ｂ）が新規である場合にのみ、当該セキュリティ情報を開発元クライアント３００へ転送するようにしたので、不要なセキュリティ情報を開発元クライアント３００へ転送するという無駄を防止でき、効率良くセキュリティ情報の収集を行うことできる。

【００８０】

（実施の形態３）

図８は、本発明にかかる実施の形態３の構成を示すブロック図である。この図において、ユーザクライアント５０１は、ユーザ５００により操作されるコンピュータ端末であり、ネットワーク５０２を介してセキュリティ情報仲介装置６００にアクセス可能とされている。

【００８１】

ユーザ５００は、後述する開発元７０１Ａおよび７０１Ｂ、その他の開発元により開発された各種コンピュータプログラムを利用する者である。また、ユーザ５００は、コンピュータプログラムのバグ等のセキュリティホールを発見し、これをセキュリティ情報として提供することができる知識を有するものである。

【００８２】

また、ユーザクライアント５０１は、ユーザクライアント１１（図１参照）と同様にして、ネットワーク５０２を介してセキュリティ情報仲介装置６００にセキュリティ情報８００を登録する機能と、セキュリティ情報仲介装置６００からの情報（同図では、返答情報８０１および支払情報８０２）を受信する機能とを

備えている。

【００８３】

上記セキュリティ情報８００は、ユーザ５００がコンピュータプログラムにセキュリティホールを発見した場合に、当該コンピュータプログラムの開発元へ提供される情報であり、セキュリティ情報４０（図２（ａ）参照）と同一の構成とされている。具体的には、図９（ａ）に示したセキュリティ情報８００は、「登録者」（ユーザ５００）および「セキュリティ情報の内容」（ソフトウェアＸのバグ問題）から構成されている。

【００８４】

返答情報８０１は、返答情報４１Ａ（図２（ｂ）参照）と同様にして、セキュリティ情報８００が有効であると開発元に判断された場合に、当該開発元からユーザ５００へ返答される情報である。具体的には、図９（ｂ）に示した返答情報８０１は、「返答者」（開発元７０１Ａ）、「判定結果」（有効）、「登録者」（ユーザ５００）、「分類」（Ａ）および「セキュリティ情報の内容」（ソフトウェアＸのバグ問題）から構成されている。上記「分類」は、当該セキュリティ情報の内容が該当する分類項目を表す情報である。

【００８５】

支払情報８０２は、支払情報４２（図２（ｄ）参照）と同様にして、開発元７０１Ａ側でセキュリティ情報８００が有効であると判断された場合に、セキュリティ情報８００を提供した代償として、開発元７０１Ａからユーザ５００へ支払われる金額や、支払い方法等に関する情報である。具体的には、図９（ｃ）に示した支払情報８０２は、「支払金額」（１００００円）、「支払先」（ユーザ５００）、「支払者」（開発元７０１Ａ）および「支払方法」（電子決済）から構成されている。

【００８６】

セキュリティ情報仲介装置６００は、ユーザ５００と、開発元７０１Ａおよび７０１Ｂとの間においてセキュリティ情報を仲介するサーバであり、ネットワーク５０２とネットワーク７０２との間に介挿されている。このセキュリティ情報仲介装置６００には、ユーザクライアント５０１、開発元クライアント７００Ａ

および７００Ｂがアクセスする。

【００８７】

セキュリティ情報仲介装置６００において、受信部６０１は、ユーザクライアント５０１からのセキュリティ情報８００を受信する機能を備えている。情報管理部６０２は、受信部６０１に受信されたセキュリティ情報８００や、後述する受信部６０７に受信された返答情報８０１および支払情報８０２を管理する機能を備えている。この情報管理部６０２の機能については、後述する。

【００８８】

転送部６０５は、情報管理部６０２により登録されたセキュリティ情報を、ネットワーク７０２を介して開発元クライアント７００Ａおよび７００Ｂの双方に転送する機能を備えている。また、転送部６０５は、開発元クライアント７００Ａおよび７００Ｂからの分類情報８０３Ａおよび８０３Ｂを受信し、これらを分類情報データベース６０６に登録する機能も備えている。

【００８９】

分類情報８０３Ａは、開発元７０１Ａで必要とするセキュリティ情報の分類を表す情報である。具体的には、図９（ｄ）に示した分類情報８０３Ａは、「開発元」（開発元７０１Ａ）および「分類」（Ａ）から構成されている。従って、開発元７０１Ａは、分類「Ａ」に属するセキュリティ情報のみが必要であって、その他の分類に属するセキュリティ情報を必要としていない。つまり、分類情報８０３Ａは、セキュリティ情報仲介装置６００に登録される多数のセキュリティ情報の中から、開発元７０１Ａで必要とするセキュリティ情報を抽出するためのフィルタリング情報である。

【００９０】

一方、分類情報８０３Ｂは、分類情報８０３Ａと同様にして、開発元７０１Ｂで必要とするセキュリティ情報の分類を表す情報である。具体的には、図９（ｅ）に示した分類情報８０３Ｂは、「開発元」（開発元７０１Ｂ）および「分類」（Ｂ）から構成されている。

【００９１】

従って、開発元７０１Ｂは、分類「Ｂ」に属するセキュリティ情報のみが必要

であって、その他の分類に属するセキュリティ情報を必要としていない。このように、分類情報８０３Ｂも、分類情報８０３Ａと同様にして、セキュリティ情報仲介装置６００に登録される多数のセキュリティ情報の中から、開発元７０１Ｂで必要とするセキュリティ情報を抽出するためのフィルタリング情報である。

【００９２】

また、分類情報データベース６０６は、図１０（ｃ）に示したように、「開発元」および「分類」から構成されている。この分類情報データベース６０６において、「開発元」（＝開発元７０１Ａ）のレコードは、分類情報８０３Ａ（図９（ｄ）参照）に対応しており、「開発元」（＝開発元７０１Ｂ）のレコードは、分類情報８０３Ｂ（図９（ｅ）参照）に対応している。

【００９３】

ネットワーク７０２は、セキュリティ情報仲介装置６００と開発元クライアント７００Ａおよび７００Ｂとを接続するものである。開発元クライアント７００Ａは、コンピュータプログラムのベンダである開発元７０１Ａ側に設置されたコンピュータ端末である。開発元クライアント７００Ｂは、コンピュータプログラムのベンダである開発元７０１Ｂ側に設置されたコンピュータ端末である。

【００９４】

開発元クライアント７００Ａは、分類情報８０３Ａ（図９（ｄ）参照）を転送部６０５へ送信し、また、上記分類情報８０３Ａに対応するセキュリティ情報（同図では、セキュリティ情報８００）を受信する。また、開発元クライアント７００Ａは、当該セキュリティ情報が有効である場合、上述した返答情報８０１（図９（ｂ）参照）および支払情報８０２（図９（ｃ）参照）をセキュリティ情報仲介装置６００へ送信する。

【００９５】

一方、開発元クライアント７００Ｂは、分類情報８０３Ｂ（図９（ｅ）参照）を転送部６０５へ送信し、また、上記分類情報８０３Ｂに対応するセキュリティ情報を受信する。また、開発元クライアント７００Ｂは、開発元クライアント７００Ａと同様にして、当該セキュリティ情報が有効である場合、返答情報および支払情報をセキュリティ情報仲介装置６００へ送信する。

【００９６】

セキュリティ情報仲介装置６００において、受信部６０７は、開発元クライアント７００Ａ、７００Ｂからネットワーク７０２を介して送信される返答情報、支払情報（同図では、返答情報８０１および支払情報８０２）を受信する機能を備えている。情報管理部６０２は、受信部６０１に受信されたセキュリティ情報（同図では、セキュリティ情報８００）を図１０（ａ）に示したセキュリティ情報データベース６０３に登録する機能を備えている。

【００９７】

このセキュリティ情報データベース６０３は、セキュリティ情報に対して登録順に付与される「登録番号」、「登録日時」、「登録者」、セキュリティ情報の分類を表す「分類」、および「セキュリティ情報の内容」から構成されている。同図において、「登録番号」＝「３」のレコードは、セキュリティ情報８００（図９（ａ）参照）に対応している。

【００９８】

また、情報管理部６０２は、受信部６０７に受信された返答情報（同図では、返答情報８０１）を図１０（ｂ）に示した返答情報データベース６０４に登録する機能を備えている。この返答情報データベース６０４は、返答情報に対して登録順に付与される「返答番号」、「返答日時」、「登録番号」（図１０（ａ）参照）、「返答者」、「分類」（図１０（ａ）参照）および「判定結果」から構成されている。同図において、「返答番号」＝「３」のレコードは、返答情報８０１（図９（ｂ）参照）に対応している。

【００９９】

さらに、情報管理部６０２は、「判定結果」が「有効」または「無効」とされた返答情報（同図では返答情報８０１）と、支払情報（同図では支払情報８０２）とを転送部６０８へ渡す。転送部６０８は、情報管理部６０２からの返答情報、支払情報を当該ユーザクライアントへネットワーク５０２を介して転送する機能を備えている。

【０１００】

つぎに、実施の形態３の動作について、図１１に示したフローチャートを参照

しつつ説明する。同図に示したステップＳＣ１では、転送部６０５は、分類情報登録処理を実行する。具体的には、転送部６０５は、開発元クライアント７００Ａおよび７００Ｂからネットワーク７０２を介して、分類情報８０３Ａ（図９（ｄ）参照）および分類情報８０３Ｂ（図９（ｅ）参照）を受信すると、これらを分類情報データベース６０６（図１０（ｃ）参照）に登録する。

【０１０１】

上記分類情報登録処理が終了すると、ステップＳＣ２では、情報管理部６０２は、受信部６０１によりセキュリティ情報が受信されたか否かを判断し、この場合、判断結果を「Ｎｏ」として同判断を繰り返す。ここで、ソフトウェアＸのバグ（セキュリティホール）を発見したユーザ５００は、図９（ａ）に示したセキュリティ情報８００をユーザクライアント５０１により作成する。つぎに、ユーザ５００の操作により、ユーザクライアント５０１からセキュリティ情報仲介装置６００へセキュリティ情報８００が送信される。

【０１０２】

そして、上記セキュリティ情報８００が受信部６０１に受信されると、情報管理部６０２は、ステップＳＣ２の判断結果を「Ｙｅｓ」とする。ステップＳＣ３では、情報管理部６０２は、セキュリティ情報８００の「登録者」および「セキュリティ情報の内容」をキーとして、図１０（ａ）に示したセキュリティ情報データベース６０３を検索する。この場合、セキュリティ情報データベース６０３には、「登録番号」＝１および２のレコードのみが存在しているものとする。

【０１０３】

ステップＳＣ４では、情報管理部６０２は、検索ヒットしたか否か、すなわち、セキュリティ情報８００と同一の内容がセキュリティ情報データベース６０３に登録されているか否かを判断し、この判断結果が「Ｙｅｓ」である場合、ステップＳＣ１５では、情報管理部６０２は、登録拒絶をする。この場合、情報管理部６０２は、ステップＳＣ４の判断結果を「Ｎｏ」とする。

【０１０４】

ステップＳＣ５では、情報管理部６０２は、受信されたセキュリティ情報８００の内容に基づいて、当該セキュリティ情報８００が、予め設定された分類（例

えば、Ａ～Ｚ）のうち、どの分類に当てはまるかを判断する分類処理を実行する。

【０１０５】

この場合、情報管理部６０２は、セキュリティ情報８００の分類をＡと判断したものとする。ステップＳＣ６では、情報管理部６０２は、セキュリティ情報８００を分類Ａに対応付けて、セキュリティ情報データベース６０３（図１０（ａ）参照）に登録する。これにより、セキュリティ情報データベース６０３には、「登録番号」＝３のレコード（セキュリティ情報８００に対応）が追加される。

【０１０６】

ステップＳＣ７では、情報管理部６０２は、転送部６０５を経由して分類情報データベース６０６にアクセスした後、セキュリティ情報８００の分類Ａをキーとして図１０（ｃ）に示した分類情報データベース６０６を検索する。ステップＳＣ８では、情報管理部６０２は、セキュリティ情報８００の分類Ａと同一の分類が分類情報データベース６０６に存在するか否かを判断する。

【０１０７】

この場合、分類情報データベース６０６における「開発元」（＝開発元７０１Ａ）の分類（＝Ａ）がセキュリティ情報８００の分類Ａと一致しているため、情報管理部６０２は、ステップＳＣ８の判断結果を「Ｙｅｓ」とする。なお、ステップＳＣ８の判断結果が「Ｎｏ」である場合、情報管理部６０２は、ステップＳＣ２以降の処理を繰り返す。

【０１０８】

ステップＳＣ９では、情報管理部６０２は、開発元クライアント７００Ａ宛のセキュリティ情報８００を転送部６０５へ渡す。これにより、転送部６０５は、セキュリティ情報８００を開発元クライアント７００Ａに転送する。この場合、開発元クライアント７００Ｂには、セキュリティ情報８００が転送されない。ステップＳＣ１０では、情報管理部６０２は、受信部６０７により返答情報が受信されたか否かを判断し、この場合、判断結果を「Ｎｏ」として同判断を繰り返す。

【０１０９】

そして、開発元クライアント７００Ａによりセキュリティ情報８００が受信されると、開発元７０１Ａは、セキュリティ情報８００が有効な情報であるか否かを判断する。この場合、開発元７０１Ａでは、セキュリティ情報８００が有効であると判断されたものとする。開発元７０１Ａでは、開発元クライアント７００Ａを用いて、返答情報８０１（図９（ｂ）参照）および支払情報８０２（図９（ｃ）参照）を作成した後、これらをセキュリティ情報仲介装置６００宛に送信する。これらの返答情報８０１および支払情報８０２は、ネットワーク７０２を介してセキュリティ情報仲介装置６００の受信部６０７に受信される。

【０１１０】

これにより、情報管理部６０２は、ステップＳＣ１０の判断結果を「Ｙｅｓ」とする。ステップＳＣ１１では、情報管理部６０２は、返答情報８０１を返答情報データベース６０４（図１０（ｂ）参照）に登録する。これにより、返答情報データベース６０４には、「返答番号」＝３のレコード（返答情報８０１に対応）が追加される。

【０１１１】

ステップＳＣ１２では、情報管理部６０２は、図９（ｂ）に示した返答情報８０１の「判定結果」が有効であるか否かを判断し、この場合、判断結果を「Ｙｅｓ」とする。ステップＳＣ１３では、情報管理部６０２は、返答情報８０１に対応する支払情報８０２が受信部６０７に受信されたか否かを判断し、この場合、判断結果を「Ｙｅｓ」とする。なお、ステップＳＣ１３の判断結果が「Ｎｏ」である場合、情報管理部６０２は、同判断を繰り返す。

【０１１２】

ステップＳＣ１４では、情報管理部６０２は、返答情報８０１および支払情報８０２を転送部６０８へ渡す。これにより、転送部６０８は、返答情報８０１および支払情報８０２をネットワーク５０２を介してユーザクライアント５０１へ転送する。

【０１１３】

これらの返答情報８０１および支払情報８０２がユーザクライアント５０１に受信されると、ユーザクライアント５０１は、返答情報８０１および支払情報８

０２をユーザ５００に報知する。これにより、ユーザ５００は、自身が提供したセキュリティ情報８００が有用であったことを認識するとともに、電子決済により開発元７０１Ａから１００００円が支払われることを認識する。

【０１１４】

一方、ステップＳＣ１２の判断結果が「Ｎｏ」である場合、すなわち、「判定結果」＝「無効」の返答情報が受信部６０７に受信された場合、ステップＳＣ１６では、情報管理部６０２は、拒絶メッセージとしての返答情報を転送部６０８へ渡す。これにより、転送部６０８は、返答情報（拒絶メッセージ）をネットワーク５０２を介してユーザクライアント５０１へ転送する。この返答情報（拒絶メッセージ）がユーザクライアント５０１に受信されると、ユーザクライアント５０１は、該返答情報をユーザ５００に報知する。これにより、ユーザ５００は、自身が提供したセキュリティ情報が無効であったことを認識する。

【０１１５】

以上説明したように、実施の形態３によれば、開発元７０１Ａおよび開発元７０１Ｂが所望するセキュリティ情報の分類情報を分類情報データベース６０６に登録しておき、上記分類情報と、ユーザ５００から提供されたセキュリティ情報８００の分類結果とが一致する場合にのみ当該セキュリティ情報８００を例えば開発元クライアント７００Ａへ転送するようにしたので、不要なセキュリティ情報を転送するという無駄を防止でき、さらに効率良くセキュリティ情報の収集を行うことができる。

【０１１６】

（実施の形態４）

さて、前述した実施の形態３では、当事者間（ユーザおよび開発元）でセキュリティ情報を共有する例について説明したが、セキュリティ情報や、当該コンピュータプログラムを修正するためのパッチ情報を第三者である一般ユーザに公開するようにしてもよい。以下では、この場合を実施の形態４として説明する。

【０１１７】

図１２は、本発明にかかる実施の形態４の構成を示すブロック図である。この図において、図８の各部に対応する部分には同一の符号を付ける。図１２では、

図８に示したセキュリティ情報仲介装置６００に代えてセキュリティ情報仲介装置１０００が設けられている。

【０１１８】

このセキュリティ情報仲介装置１０００においては、図８に示した情報管理部６０２および返答情報データベース６０４に代えて、情報管理部１００１および返答情報データベース１００２が設けられている。さらに、セキュリティ情報仲介装置１０００においては、情報公開部１００３および公開情報データベース１００４が新たに設けられている。また、図１２においては、ユーザ９００により操作されるユーザクライアント９０１が新たに設けられている。

【０１１９】

セキュリティ情報仲介装置１０００は、ユーザ５００および９００と、開発元７０１Ａおよび７０１Ｂとの間においてセキュリティ情報やパッチ情報を仲介するサーバであり、ネットワーク５０２とネットワーク７０２との間に介挿されている。このセキュリティ情報仲介装置１０００には、ユーザクライアント５０１、ユーザクライアント９０１、開発元クライアント７００Ａおよび７００Ｂがアクセスする。

【０１２０】

セキュリティ情報仲介装置１０００において、受信部６０７は、前述した返答情報８０１および支払情報８０２に加えて、パッチ情報１１００を開発元クライアント７００Ａより受信する。このパッチ情報１１００は、図１３（ｃ）に示したように、返答情報８０１に対応する「返答番号」（３）、「返答者」（開発元７０１Ａ）およびパッチプログラムから構成されており、セキュリティホールを有する当該コンピュータプログラムを修正するための情報である。

【０１２１】

情報管理部１００１は、受信部６０１に受信されたセキュリティ情報（同図ではセキュリティ情報８００）をセキュリティ情報データベース６０３に登録する機能を備えている。また、情報管理部１００１は、受信部６０７に受信された返答情報（同図では、返答情報８０１）を図１３（ａ）に示した返答情報データベース１００２に登録する機能を備えている。

【０１２２】

この返答情報データベース１００２は、返答情報データベース６０４（図１０（ｂ）参照）と同様にして、返答情報に対して登録順に付与される「返答番号」、「返答日時」、「登録番号」、「返答者」、「分類」および「判定結果」のカラムを備えている。さらに、返答情報データベース１００２は、「修正方法」のカラムも備えている。この「修正方法」は、セキュリティホールを有するコンピュータプログラムに対する修正方法（例えば、パッチ）を表す情報である。同図において、「返答番号」＝「３」のレコードは、返答情報８０１（図９（ｂ）参照）に対応している。

【０１２３】

また、情報管理部１００１は、情報管理部６０２と同様にして、「判定結果」が「有効」または「無効」とされた返答情報（同図では返答情報８０１）と、支払情報（同図では支払情報８０２）とを転送部６０８へ渡す。さらに、情報管理部１００１は、セキュリティ情報、返答情報およびパッチ情報を情報公開部１００３へ渡す。

【０１２４】

情報公開部１００３は、ｗｅｂサイト上の情報公開画面１２００（図１４参照）等を介して、第三者であるユーザ９００のユーザクライアント９０１に対して、セキュリティ情報、返答情報およびパッチ情報を公開する機能を備えている。また、情報公開部１００３は、情報管理部１００１からの返答情報、セキュリティ情報およびパッチ情報を、図１３（ｂ）に示した公開情報データベース１００４に登録する。

【０１２５】

この公開情報データベース１００４は、返答情報データベース１００２（図１３（ａ）参照）と同様にして、「返答番号」、「分類」、「セキュリティ情報の内容」、「返答者」、「修正方法」、「セキュリティ情報ポインタ」および「パッチ情報ポインタ」から構成されている。「セキュリティ情報ポインタ」は、セキュリティ情報が実際に格納されている領域を表すポインタであり、「パッチ情報ポインタ」は、パッチ情報が実際に格納されている領域を表すポインタである

【０１２６】

つぎに、実施の形態４の動作について、図１５に示したフローチャートを参照しつつ説明する。同図に示したステップＳＤ１では、転送部６０５は、ステップＳＣ１（図１１参照）と同様にして、分類情報８０３Ａ（図９（ｄ）参照）および分類情報８０３Ｂ（図９（ｅ）参照）を分類情報データベース６０６（図１０（ｃ）参照）に登録する。

【０１２７】

ステップＳＤ２では、情報管理部１００１は、受信部６０１によりセキュリティ情報が受信されたか否かを判断し、この場合、判断結果を「Ｎｏ」として同判断を繰り返す。ここで、ソフトウェアＸのバグ（セキュリティホール）を発見したユーザ５００は、図９（ａ）に示したセキュリティ情報８００をユーザクライアント５０１により作成する。つぎに、ユーザ５００の操作により、ユーザクライアント５０１からセキュリティ情報仲介装置１０００へセキュリティ情報８００が送信される。

【０１２８】

そして、上記セキュリティ情報８００が受信部６０１に受信されると、情報管理部１００１は、ステップＳＤ２の判断結果を「Ｙｅｓ」とする。ステップＳＤ３では、情報管理部１００１は、セキュリティ情報８００の「登録者」および「セキュリティ情報の内容」をキーとして、図１０（ａ）に示したセキュリティ情報データベース６０３を検索する。この場合、セキュリティ情報データベース６０３には、「登録番号」＝１および２のレコードのみが存在しているものとする。

【０１２９】

ステップＳＤ４では、情報管理部１００１は、検索ヒットしたか否か、すなわち、セキュリティ情報８００と同一の内容がセキュリティ情報データベース６０３に登録されているか否かを判断し、この判断結果が「Ｙｅｓ」である場合、ステップＳＤ１９では、情報管理部１００１は、登録拒絶をする。この場合、情報管理部１００１は、ステップＳＤ４の判断結果を「Ｎｏ」とする。

【０１３０】

ステップＳＤ５では、情報管理部１００１は、受信されたセキュリティ情報８００の内容に基づいて、当該セキュリティ情報８００が、予め設定された分類（例えば、Ａ～Ｚ）のうち、どの分類に当てはまるかを判断する分類処理を実行する。

【０１３１】

この場合、情報管理部１００１は、セキュリティ情報８００の分類をＡと判断したものとする。ステップＳＤ６では、情報管理部１００１は、セキュリティ情報８００を分類Ａに対応付けて、セキュリティ情報データベース６０３（図１０（ａ）参照）に登録する。これにより、セキュリティ情報データベース６０３には、「登録番号」＝３のレコード（セキュリティ情報８００に対応）が追加される。また、情報管理部１００１は、セキュリティ情報８００を情報公開部１００３に渡す。これにより、情報公開部１００３は、セキュリティ情報８００を公開情報データベース１００４に登録する。

【０１３２】

ステップＳＤ７では、情報管理部１００１は、転送部６０５を経由して分類情報データベース６０６にアクセスした後、セキュリティ情報８００の分類Ａをキーとして図１０（ｃ）に示した分類情報データベース６０６を検索する。ステップＳＤ８では、情報管理部１００１は、セキュリティ情報８００の分類Ａと同一の分類が分類情報データベース６０６に存在するか否かを判断する。

【０１３３】

この場合、分類情報データベース６０６における「開発元」（＝開発元７０１Ａ）の分類（＝Ａ）がセキュリティ情報８００の分類Ａと一致しているため、情報管理部１００１は、ステップＳＤ８の判断結果を「Ｙｅｓ」とする。なお、ステップＳＤ４の判断結果が「Ｎｏ」である場合、情報管理部１００１は、ステップＳＤ２以降の処理を繰り返す。

【０１３４】

ステップＳＤ９では、情報管理部１００１は、開発元クライアント７００Ａ宛のセキュリティ情報８００を転送部６０５へ渡す。これにより、転送部６０５は

、セキュリティ情報８００を開発元クライアント７００Ａに転送する。この場合、開発元クライアント７００Ｂには、セキュリティ情報８００が転送されない。ステップＳＤ１０では、情報管理部１００１は、受信部６０７により返答情報が受信されたか否かを判断し、この場合、判断結果を「Ｎｏ」として同判断を繰り返す。

【０１３５】

そして、開発元クライアント７００Ａによりセキュリティ情報８００が受信されると、開発元７０１Ａは、セキュリティ情報８００が有効な情報であるか否かを判断する。この場合、開発元７０１Ａでは、セキュリティ情報８００が有効であると判断されたものとする。開発元７０１Ａでは、開発元クライアント７００Ａを用いて、返答情報８０１（図９（ｂ）参照）、支払情報８０２（図９（ｃ）参照）およびパッチ情報１１００（図１３（ｃ）参照）を作成した後、これらをセキュリティ情報仲介装置１０００宛に送信する。これらの返答情報８０１、支払情報８０２およびパッチ情報１１００は、ネットワーク７０２を介してセキュリティ情報仲介装置１０００の受信部６０７に受信される。

【０１３６】

これにより、情報管理部１００１は、ステップＳＤ１０の判断結果を「Ｙｅｓ」とする。ステップＳＤ１１では、情報管理部１００１は、受信部６０７にパッチ情報が受信されたか否かを判断し、この場合、判断結果を「Ｙｅｓ」とする。ステップＳＤ１７では、情報管理部１００１は、返答情報８０１およびパッチ情報１１００を返答情報データベース１００２（図１３（ａ）参照）に登録する。

【０１３７】

また、情報管理部１００１は、返答情報８０１およびパッチ情報１１００を情報公開部１００３に渡す。これにより、情報公開部１００３は、返答情報８０１およびパッチ情報１１００を公開情報データベース１００４（図１３（ｂ）参照）に登録する。一方、ステップＳＤ１１の判断結果が「Ｎｏ」である場合、情報管理部１００１は、返答情報８０１を返答情報データベース１００２（図１３（ａ）参照）に登録する。

【０１３８】

ステップＳＤ１３では、情報管理部１００１は、図９（ｂ）に示した返答情報８０１の「判定結果」が有効であるか否かを判断し、この場合、判断結果を「Ｙｅｓ」とする。ステップＳＤ１４では、情報管理部１００１は、返答情報８０１に対応する支払情報８０２が受信部６０７に受信されたか否かを判断し、この場合、判断結果を「Ｙｅｓ」とする。なお、ステップＳＤ１４の判断結果が「Ｎｏ」である場合、情報管理部１００１は、同判断を繰り返す。

【０１３９】

ステップＳＤ１５では、情報管理部１００１は、返答情報８０１および支払情報８０２を転送部６０８へ渡す。これにより、転送部６０８は、返答情報８０１および支払情報８０２をネットワーク５０２を介してユーザクライアント５０１へ転送する。

【０１４０】

これらの返答情報８０１および支払情報８０２がユーザクライアント５０１に受信されると、ユーザクライアント５０１は、返答情報８０１および支払情報８０２をユーザ５００に報知する。これにより、ユーザ５００は、自身が提供したセキュリティ情報８００が有用であったことを認識するとともに、電子決済により開発元７０１Ａから１００００円が支払われることを認識する。

【０１４１】

一方、ステップＳＤ１３の判断結果が「Ｎｏ」である場合、すなわち、「判定結果」＝「無効」の返答情報が受信部６０７に受信された場合、ステップＳＤ１８では、情報管理部１００１は、拒絶メッセージとしての返答情報を転送部６０８へ渡す。これにより、転送部６０８は、返答情報（拒絶メッセージ）をネットワーク５０２を介してユーザクライアント５０１へ転送する。この返答情報（拒絶メッセージ）がユーザクライアント５０１に受信されると、ユーザクライアント５０１は、該返答情報をユーザ５００に報知する。これにより、ユーザ５００は、自身が提供したセキュリティ情報が無効であったことを認識する。

【０１４２】

つぎに、図１２に示した情報公開部１００３の動作について、図１６に示したフローチャートを参照しつつ説明する。ステップＳＥ１では、情報公開部１００

３は、情報管理部１００１からの公開情報（セキュリティ情報、返答情報、パッチ情報）を受信したか否かを判断し、この判断結果が「Ｙｅｓ」である場合、ステップＳＥ２で公開情報データベース１００４を更新する。

【０１４３】

一方、ステップＳＥ１の判断結果が「Ｎｏ」である場合、ステップＳＥ３では、情報公開部１００３は、ユーザクライアント（同図ではユーザクライアント９０１）からアクセス要求があるか否かを判断し、この場合、同判断結果が「Ｎｏ」であるものとすると、ステップＳＥ１以降の処理を繰り返す。ここで、ユーザクライアント９０１よりアクセス要求があると、情報公開部１００３は、ステップＳＥ３の判断結果を「Ｙｅｓ」とする。

【０１４４】

ステップＳＥ４では、情報公開部１００３は、公開情報データベース１００４（図１３（ｂ）参照）に基づいて、図１４に示した情報公開画面１２００をユーザクライアント９０１の表示部（図示略）に表示させる処理を実行する。この情報公開画面１２００は、ユーザ９００にセキュリティ情報（「返答情報」、「分類」、「セキュリティ情報の内容」、「返答者」および「修正方法」）を公開するための画面である。

【０１４５】

ステップＳＥ５では、情報公開部１００３は、ユーザ９００により、情報公開画面１２００の中から所望のセキュリティ情報が選択されたか否かを判断し、この場合、判断結果が「Ｎｏ」であるものとする。ステップＳＥ８では、情報公開部１００３は、アクセス解除されたか否か、具体的には終了ボタン１２０１（図１４参照）が押下されたか否かを判断し、この場合、判断結果を「Ｎｏ」として、ステップＳＥ５以降の処理を繰り返す。

【０１４６】

ここで、ユーザ９００により、図１４に示した返答番号３が入力されることにより、返答番号「３」に対応するセキュリティ情報が選択されると、情報公開部１００３は、ステップＳＥ５の判断結果を「Ｙｅｓ」とする。ステップＳＥ６では、情報公開部１００３は、返答番号「３」をキーとして、図１３に示した公開

情報データベース１００４を検索し、セキュリティ情報ポインタ「ＰＳ３」およびパッチ情報ポインタ「ＰＰ３」を取得する。

【０１４７】

つぎに、情報公開部１００３は、セキュリティ情報ポインタ「ＰＳ３」およびパッチ情報ポインタ「ＰＰ３」に基づいて、公開情報データベース１００４からセキュリティ情報８００およびパッチ情報１１００を取得する。ステップＳＥ７では、情報公開部１００３は、上記セキュリティ情報８００およびパッチ情報１１００をネットワーク５０２を介してユーザクライアント９０１へ転送する。ここで、ユーザ９００により終了ボタン１２０１が押下されると、情報公開部１００３は、ステップＳＥ８の判断結果を「Ｙｅｓ」とし、ステップＳＥ１以降の処理を繰り返す。

【０１４８】

また、セキュリティ情報８００およびパッチ情報１１００がユーザクライアント９０１に受信されると、ユーザ９００は、セキュリティ情報８００の内容を認識し、パッチ情報１１００のパッチプログラムを「ソフトウェアＸ」に適用する。これにより、「ソフトウェアＸ」が修正される。

【０１４９】

なお、実施の形態４では、ユーザ９００が所望するクライアント情報の分類情報を予め情報公開部１００３に登録しておき、ユーザクライアント９０１からアクセス要求があった場合、当該分類情報に対応するセキュリティ情報（パッチ情報）を公開情報データベース１００４から抽出し、これをユーザ９００に対して公開するようにしてもよい。さらに、実施の形態４では、返答情報８０１および支払情報８０２に加えて、パッチ情報１１００もユーザクライアント５０１に転送するようにしてもよい。

【０１５０】

以上説明したように、実施の形態４によれば、情報公開部１００３によりセキュリティ情報を公開するようにしたので、セキュリティ情報の提供に関する第三者（ユーザ９００）の関心を引くことができ、多数のセキュリティ情報の提供を期待することができる。また、実施の形態４によれば、パッチ情報１１００をユ

ーザクライアント９０１（ユーザクライアント５０１）へ転送するようにしたので、迅速にセキュリティ情報に対する対策を講じることができる。

【０１５１】

以上本発明にかかる実施の形態１～４について図面を参照して詳述してきたが、具体的な構成例はこれら実施の形態１～４に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。

【０１５２】

例えば、前述した実施の形態１～４においては、セキュリティ情報を仲介する機能を実現するためのセキュリティ情報仲介プログラムを図１７に示したコンピュータ読み取り可能な記録媒体１４００に記録して、この記録媒体１４００に記録されたセキュリティ情報仲介プログラムを同図に示したコンピュータ１３００に読み込ませ、実行することによりセキュリティ情報の仲介を行うようにしてもよい。

【０１５３】

図１７に示したコンピュータ１３００は、上記セキュリティ情報仲介プログラムを実行するＣＰＵ１３０１と、キーボード、マウス等の入力装置１３０２と、各種データを記憶するＲＯＭ（Read Only Memory）１３０３と、演算パラメータ等を記憶するＲＡＭ（Random Access Memory）１３０４と、記録媒体１４００からセキュリティ情報仲介プログラムを読み取る読取装置１３０５と、ディスプレイ、プリンタ等の出力装置１３０６と、装置各部を接続するバスＢＵとから構成されている。

【０１５４】

ＣＰＵ１３０１は、読取装置１３０５を経由して記録媒体１４００に記録されているセキュリティ情報仲介プログラムを読み込んだ後、セキュリティ情報仲介プログラムを実行することにより、前述したセキュリティ情報の仲介を行う。なお、記録媒体１４００には、光ディスク、フロッピーディスク、ハードディスク等の可搬型の記録媒体が含まれることはもとより、ネットワークのようにデータを一時的に記録保持するような伝送媒体も含まれる。

【０１５５】

【発明の効果】

以上説明したように、本発明によれば、情報提供者からのセキュリティ情報をダイレクトに情報受信者側に提供し、しかも有用なセキュリティ情報を提供した者に対して支払いを行うようにしたので、情報提供者（ユーザ）にとってセキュリティ情報を提供し易い環境を整備し、情報受信者（例えば、開発元）にとって低コストで有用なセキュリティ情報を収集することができるという効果を奏する。

【０１５６】

また、本発明によれば、情報提供者より提供されたセキュリティ情報が新規である場合にのみ、当該セキュリティ情報を情報受信者端末へ転送するようにしたので、不要なセキュリティ情報を情報受信者端末へ転送するという無駄を防止でき、効率良くセキュリティ情報の収集を行うことできるという効果を奏する。

【０１５７】

また、本発明によれば、情報受信者が所望するセキュリティ情報の分類情報を登録しておき、上記分類情報と、提供されたセキュリティ情報の分類結果とが一致する場合にのみ当該セキュリティ情報を情報受信者端末へ転送するようにしたので、不要なセキュリティ情報を情報受信者端末へ転送するという無駄を防止でき、さらに効率良くセキュリティ情報の収集を行うことができるという効果を奏する。

【０１５８】

また、本発明によれば、情報提供者から提供されたセキュリティ情報の無効を示す無効情報を情報提供者端末へ転送するようにしたので、提供したセキュリティ情報の使われ方（有用または無効）に関心を持つ情報提供者に対するサービスを向上させることができるという効果を奏する。

【０１５９】

また、本発明によれば、有用性が示されたセキュリティ情報の対策用の修正情報を情報提供者端末へ転送するようにしたので、迅速にセキュリティ情報に対する対策を講じることができるという効果を奏する。

【０１６０】

また、本発明によれば、セキュリティ情報を公開するようにしたので、セキュリティ情報の提供に関する第三者の関心を引くことができ、多数のセキュリティ情報の提供を期待することができるという効果を奏する。

【０１６１】

また、本発明によれば、セキュリティ情報および修正情報を公開するようにしたので、セキュリティ情報の提供に関する第三者の関心を引くことができ、多数のセキュリティ情報の提供を期待することができるとともに、迅速にセキュリティ情報に対する対策を講じることができるという効果を奏する。

【図面の簡単な説明】

【図１】

本発明にかかる実施の形態１の構成を示すブロック図である。

【図２】

図１に示したセキュリティ情報４０、返答情報４１Ａ、４１Ｂおよび支払情報４２を示す図である。

【図３】

同実施の形態１の動作を説明するフローチャートである。

【図４】

本発明にかかる実施の形態２の構成を示すブロック図である。

【図５】

図４に示したセキュリティ情報４００Ａ、４００Ｂ、返答情報４０１Ａ、４０１Ｂおよび支払情報４０２を示す図である。

【図６】

図４に示したセキュリティ情報データベース２０３および返答情報データベース２０４のデータ構造を示す図である。

【図７】

同実施の形態２の動作を説明するフローチャートである。

【図８】

本発明にかかる実施の形態３の構成を示すブロック図である。

【図９】

図８に示したセキュリティ情報８００、返答情報８０１、支払情報８０２および分類情報８０３Ａ、８０３Ｂを示す図である。

【図１０】

図８に示したセキュリティ情報データベース６０３、返答情報データベース６０４および分類情報データベース６０６のデータ構造を示す図である。

【図１１】

同実施の形態３の動作を説明するフローチャートである。

【図１２】

本発明にかかる実施の形態４の構成を示すブロック図である。

【図１３】

図１２に示した返答情報データベース１００２、公開情報データベース１００４およびパッチ情報１１００のデータ構造を示す図である。

【図１４】

同実施の形態４における情報公開画面１２００の一例を示す図である。

【図１５】

同実施の形態４の動作を説明するフローチャートである。

【図１６】

図１２に示した情報公開部１００３の動作を説明するフローチャートである。

【図１７】

本発明にかかる実施の形態１～４の変形例を示すブロック図である。

【符号の説明】

１１　ユーザクライアント

２０　セキュリティ情報仲介装置

２１　セキュリティ情報登録部

２３　転送部

２６　転送部

１０１Ａ　ユーザクライアント

２００　セキュリティ情報仲介装置

２０１　受信部

２０２　情報管理部

２０５　転送部

２０６　受信部

２０７　転送部

３００　開発元クライアント

５０１　ユーザクライアント

６００　セキュリティ情報仲介装置

６０１　受信部

６０２　情報管理部

６０５　転送部

６０７　受信部

６０８　転送部

７００Ａ　開発元クライアント

９０１　ユーザクライアント

１０００　セキュリティ情報仲介装置

１００１　情報管理部

１００３　情報公開部

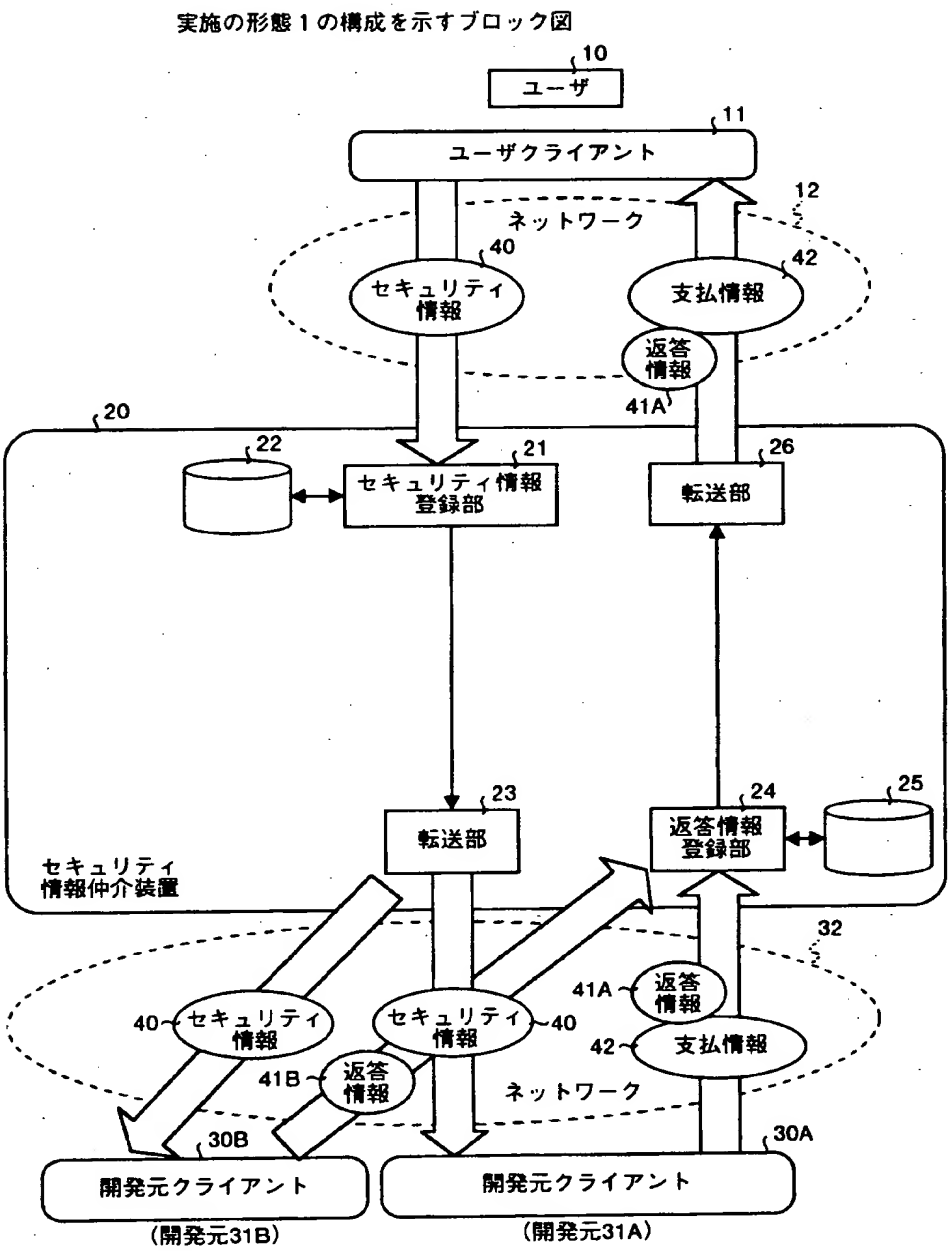
１３００　コンピュータ

１３０１　ＣＰＵ

１４００　記録媒体

【書類名】　　図面

【図１】


実施の形態１の構成を示すブロック図
10
ユーザ
11
ユーザクライアント
12
ネットワーク
40
セキュリティ情報
42
支払情報
返答情報
41A
20
22
21
セキュリティ情報登録部
26
転送部
23
転送部
24
返答情報登録部
25
セキュリティ情報仲介装置
32
41A
返答情報
40
セキュリティ情報
セキュリティ情報
40
42
支払情報
41B
返答情報
ネットワーク
30B
30A
開発元クライアント
開発元クライアント
（開発元31B）
（開発元31A）

【図２】

図１に示したセキュリティ情報40，返答情報41A，41Ｂおよび支払情報42を示す図

(a)

40；セキュリティ情報

登録者	セキュリティ情報の内容
ユーザ10	ソフトウェアＸのバグ問題

(b)

41A；返答情報

返答者	判定結果	登録者	セキュリティ情報の内容
開発元31A	有効	ユーザ10	ソフトウェアＸのバグ問題

(c)

41B；返答情報

返答者	判定結果	登録者	セキュリティ情報の内容
開発元31B	無効	ユーザ10	ソフトウェアＸのバグ問題

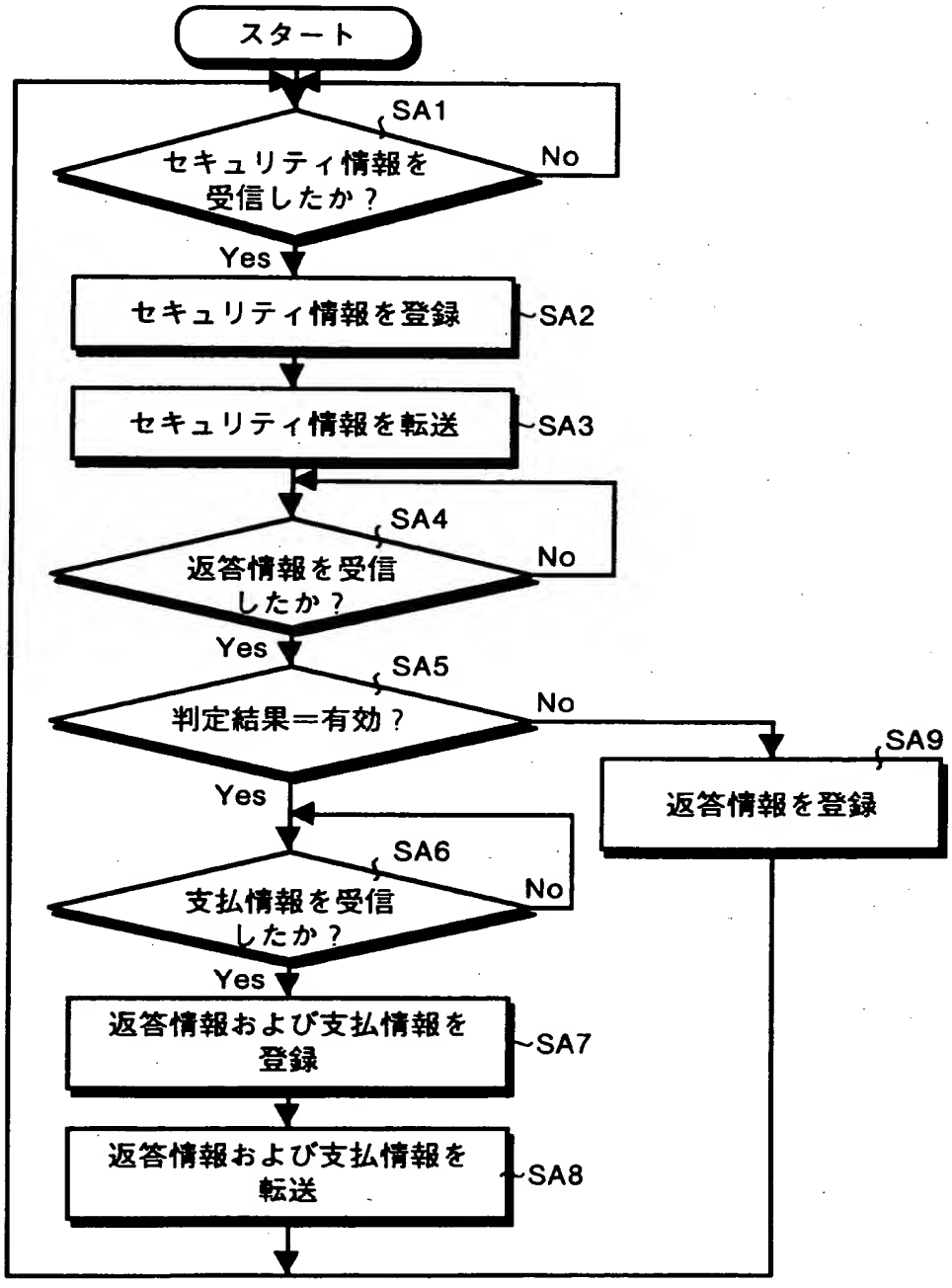
(d)

42；支払情報

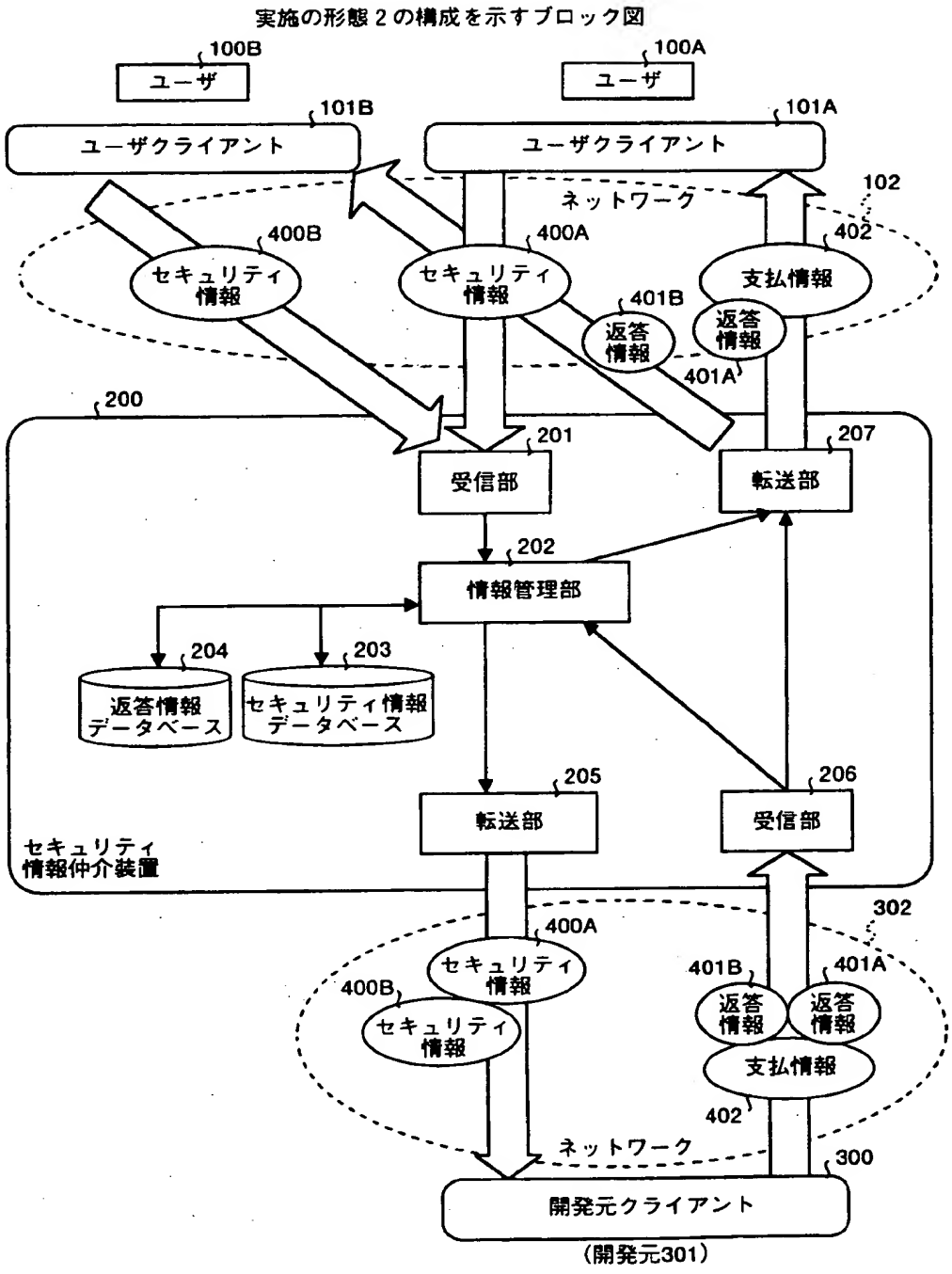
支払金額	支払先	支払者	支払方法
10000円	ユーザ10	開発元31A	電子決済

【図３】

実施の形態１の動作を説明するフローチャート



【図４】


実施の形態２の構成を示すブロック図
100B
ユーザ
100A
ユーザ
101B
ユーザクライアント
101A
ユーザクライアント
ネットワーク
102
400B
セキュリティ情報
400A
セキュリティ情報
402
支払情報
401B
返答情報
返答情報
401A
200
201
受信部
207
転送部
202
情報管理部
204
返答情報データベース
203
セキュリティ情報データベース
205
転送部
206
受信部
セキュリティ情報仲介装置
302
400A
セキュリティ情報
401B
401A
400B
セキュリティ情報
返答情報
返答情報
支払情報
402
ネットワーク
300
開発元クライアント
（開発元301）

【図５】

図４に示したセキュリティ情報400A，400B，返答情報401A，401B
および支払情報402を示す図

400A；セキュリティ情報

(a)

登録者	セキュリティ情報の内容
ユーザ100A	ソフトウェアＸのバグ問題QA

400B；セキュリティ情報

(b)

登録者	セキュリティ情報の内容
ユーザ100B	ソフトウェアＸのバグ問題QB

401A；返答情報

(c)

返答者	判定結果	登録者	セキュリティ情報の内容
開発元301	有効	ユーザ100A	ソフトウェアＸのバグ問題QA

401B；返答情報

(d)

返答者	判定結果	登録者	セキュリティ情報の内容
開発元301	無効	ユーザ100B	ソフトウェアＸのバグ問題QB

402；支払情報

(e)

支払金額	支払先	支払者	支払方法
10000円	ユーザ100A	開発元301	電子決済

【図６】

図４に示したセキュリティ情報データベース203
および返答情報データベース204のデータ構造を示す図

(a)

203；セキュリティ情報データベース

登録番号	登録日時	登録者	セキュリティ情報の内容
1	2000/4/27 18:00:13	ユーザy	ソフトウェアYのバグ問題
2	2000/5/13 14:32:10	ユーザz	ソフトウェアZのバグ問題
3	2000/6/11 19:26:30	ユーザ100A	ソフトウェアXのバグ問題QA
4	2000/7/25 08:10:40	ユーザ100B	ソフトウェアXのバグ問題QB

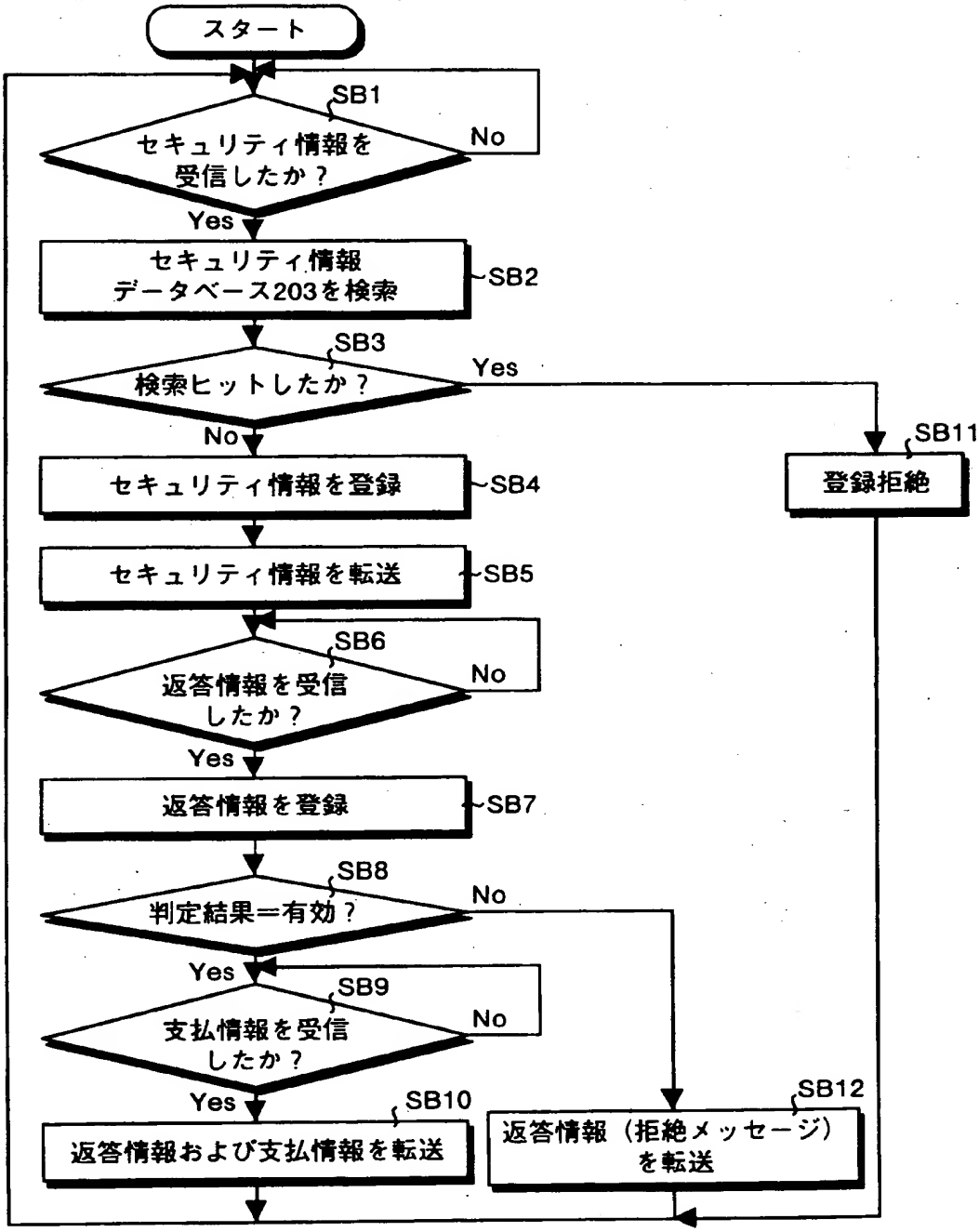
(b)

204；返答情報データベース

返答番号	返答日時	登録番号	返答者	判定結果
1	2000/4/28 12:26:14	1	開発元301	有効
2	2000/5/14 15:33:20	2	開発元301	無効
3	2000/6/12 19:36:40	3	開発元301	有効
4	2000/7/26 10:15:55	4	開発元301	無効

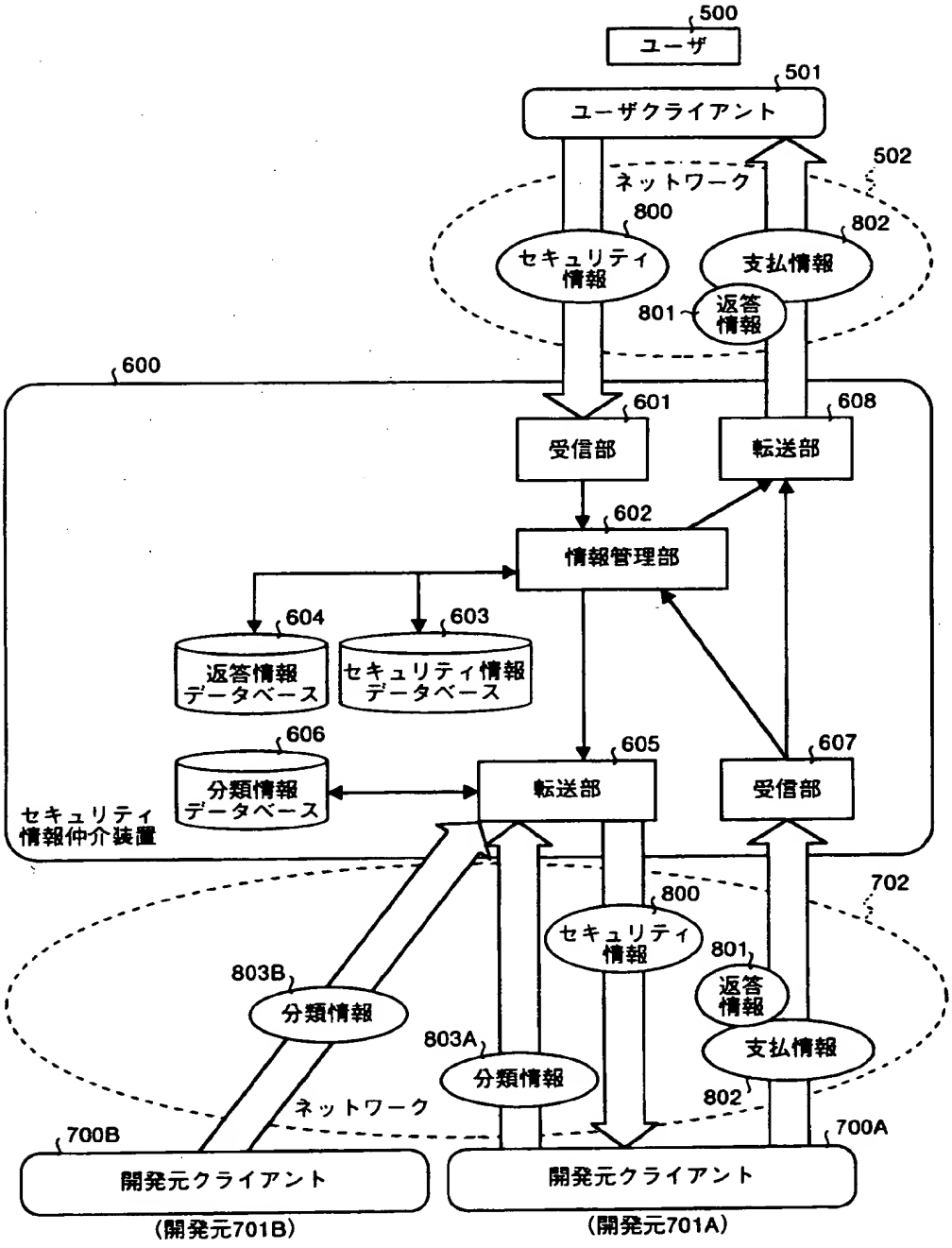
【図７】

実施の形態２の動作を説明するフローチャート



【図８】

実施の形態３の構成を示すブロック図



【図９】

図８に示したセキュリティ情報800，返答情報801，支払情報802
および分類情報803A，803Bを示す図

(a) 800；セキュリティ情報

登録者	セキュリティ情報の内容
ユーザ500	ソフトウェアＸのバグ問題

(b) 801；返答情報

返答者	判定結果	登録者	分類	セキュリティ情報の内容
開発元701A	有効	ユーザ500	A	ソフトウェアＸのバグ問題

(c) 802；支払情報

支払金額	支払先	支払者	支払方法
10000円	ユーザ500	開発元701A	電子決済

(d) 803A；分類情報

開発元	分類
開発元701A	A

(e) 803B；分類情報

開発元	分類
開発元701B	B

【図１０】

図８に示したセキュリティ情報データベース603，返答情報データベース604
および分類情報データベース606のデータ構造を示す図

(a)

603；セキュリティ情報データベース

登録番号	登録日時	登録者	分類	セキュリティ情報の内容
1	2000/4/27 18:00:13	ユーザy	B	ソフトウェアYのバグ問題
2	2000/5/13 14:32:10	ユーザz	B	ソフトウェアZのバグ問題
3	2000/6/11 19:26:30	ユーザ500	A	ソフトウェアXのバグ問題

(b)

604；返答情報データベース

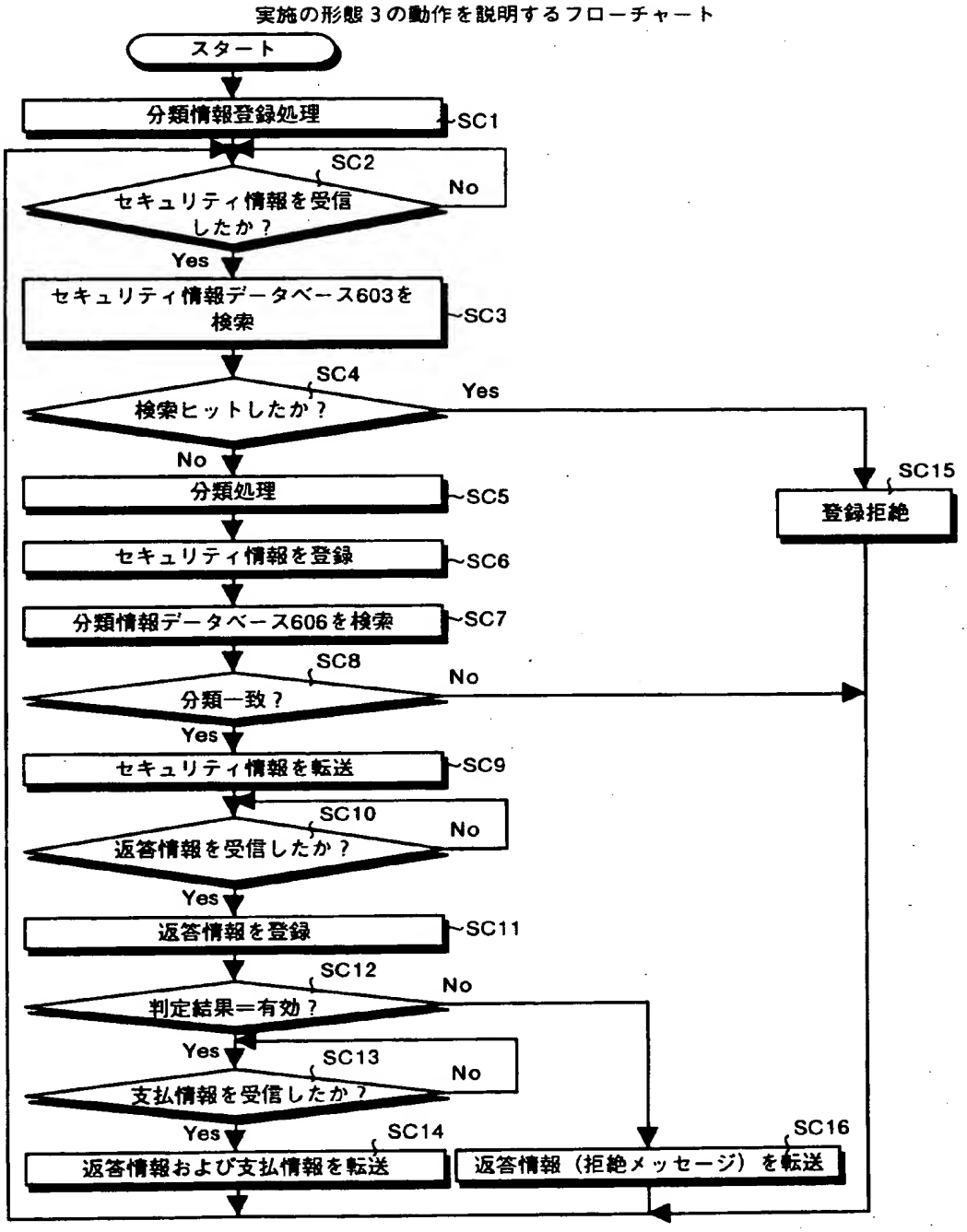
返答番号	返答日時	登録番号	返答者	分類	判定結果
1	2000/4/28 12:26:14	1	開発元701B	B	有効
2	2000/5/14 15:33:20	2	開発元701B	B	無効
3	2000/6/12 19:36:40	3	開発元701A	A	有効

(c)

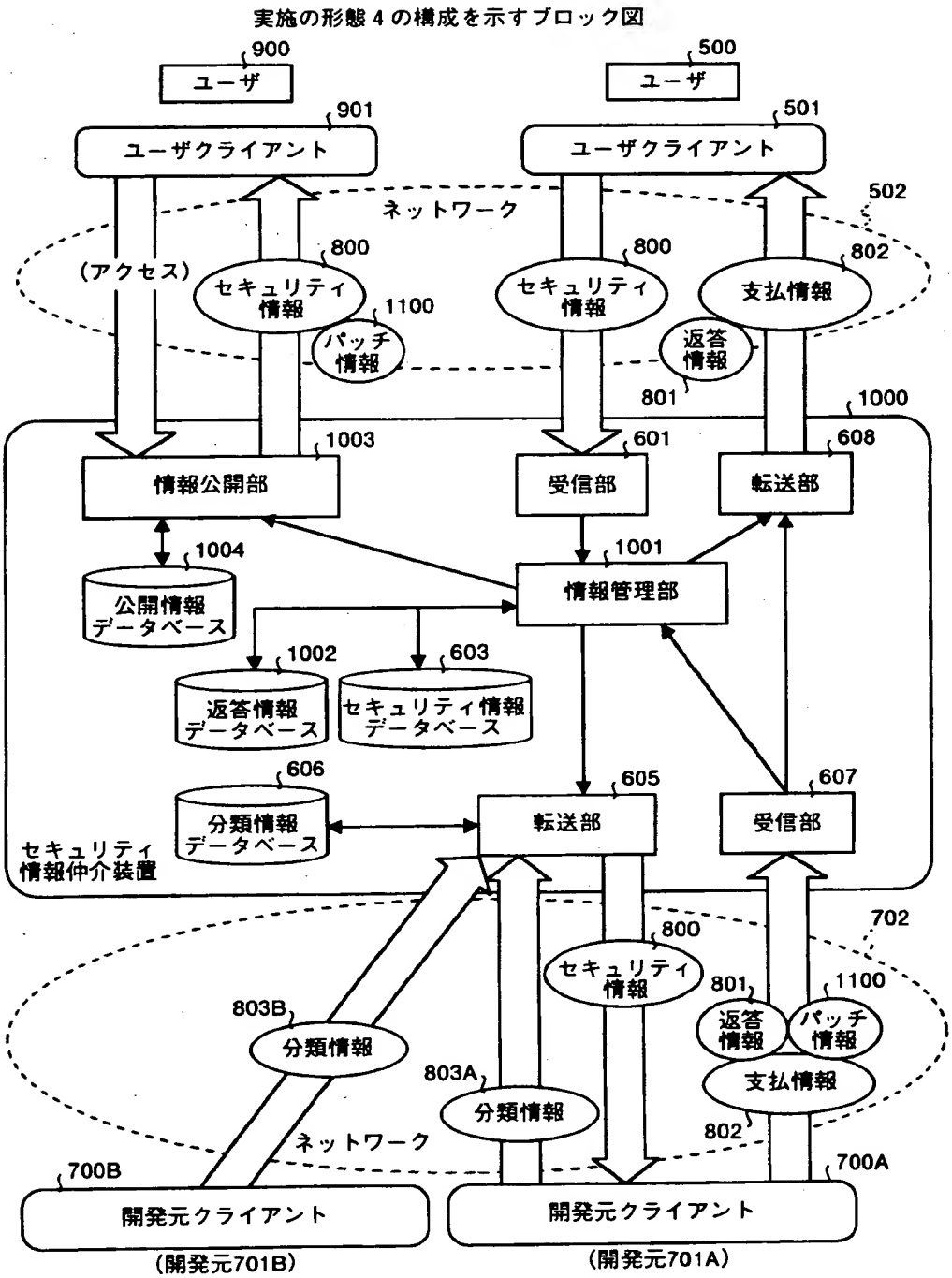
606；分類情報データベース

開発元	分類
開発元701A	A
開発元701B	B

【図１１】


実施の形態３の動作を説明するフローチャート
スタート
分類情報登録処理
SC1
SC2
セキュリティ情報を受信したか？
No
Yes
セキュリティ情報データベース603を検索
SC3
SC4
検索ヒットしたか？
Yes
No
分類処理
SC5
SC15
登録拒絶
セキュリティ情報を登録
SC6
分類情報データベース606を検索
SC7
SC8
分類一致？
No
Yes
セキュリティ情報を転送
SC9
SC10
返答情報を受信したか？
No
Yes
返答情報を登録
SC11
SC12
判定結果＝有効？
No
Yes
SC13
支払情報を受信したか？
No
Yes
SC14
返答情報および支払情報を転送
SC16
返答情報（拒絶メッセージ）を転送

【図１２】


実施の形態４の構成を示すブロック図
900
ユーザ
500
ユーザ
901
ユーザクライアント
501
ユーザクライアント
ネットワーク
502
(アクセス)
800
セキュリティ情報
1100
パッチ情報
800
セキュリティ情報
802
支払情報
返答情報
801
1000
1003
情報公開部
601
受信部
608
転送部
1004
公開情報データベース
1001
情報管理部
1002
返答情報データベース
603
セキュリティ情報データベース
606
分類情報データベース
605
転送部
607
受信部
セキュリティ情報仲介装置
702
800
セキュリティ情報
801
返答情報
1100
パッチ情報
803B
分類情報
803A
分類情報
支払情報
802
ネットワーク
700B
開発元クライアント
(開発元701B)
700A
開発元クライアント
(開発元701A)

【図１３】

図12に示した返答情報データベース1002，公開情報データベース1004
およびパッチ情報1100のデータ構造を示す図

(a)

1002；返答情報データベース

返答番号	返答日時	登録番号	返答者	分類	判定結果	修正方法
1	2000/4/28 12:26:14	1	開発元701B	B	有効	パッチ
2	2000/5/14 15:33:20	2	開発元701B	B	無効	
3	2000/6/12 19:36:40	3	開発元701A	A	有効	パッチ

(b)

1004；公開情報データベース

返答番号	分類	ｾｷｭﾘﾃｨ情報の内容	返答者	修正方法	ｾｷｭﾘﾃｨ情報ﾎﾟｲﾝﾀ	ﾊﾟｯﾁ情報ﾎﾟｲﾝﾀ
3	A	ｿﾌﾄｳｪｱXの ﾊﾞｸﾞ問題	開発元 701A	ﾊﾟｯﾁ	PS3	PP3

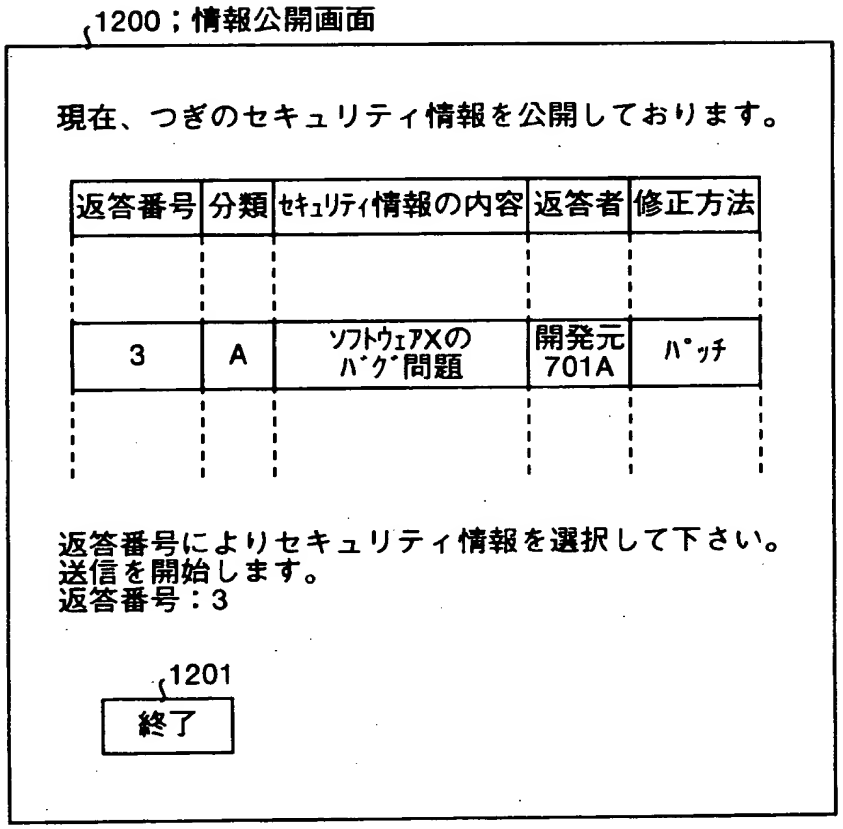
(c)

1100；パッチ情報

返答番号	返答者	
3	開発元701A	パッチプログラム

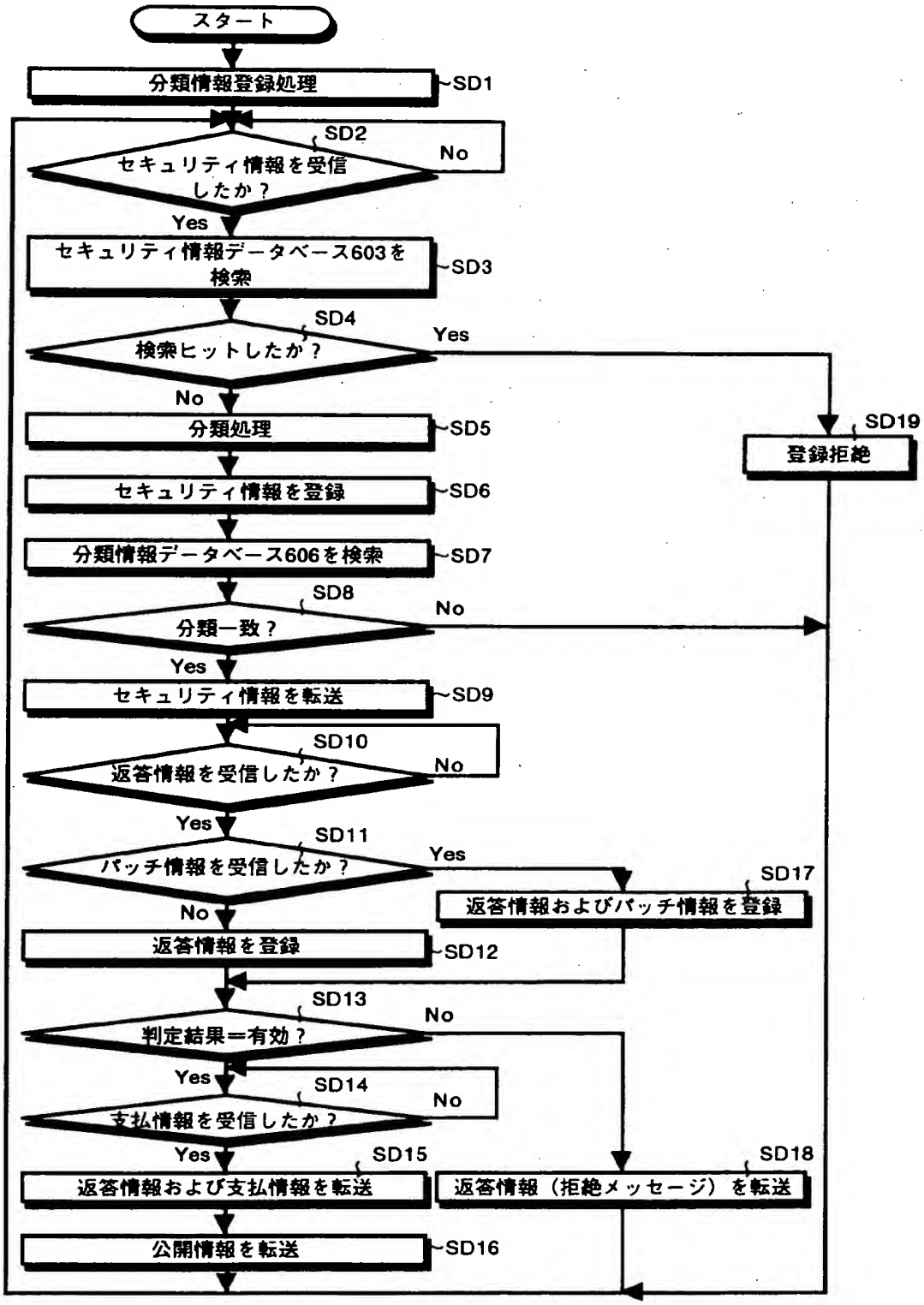
【図１４】

実施の形態４における情報公開画面1200の一例を示す図



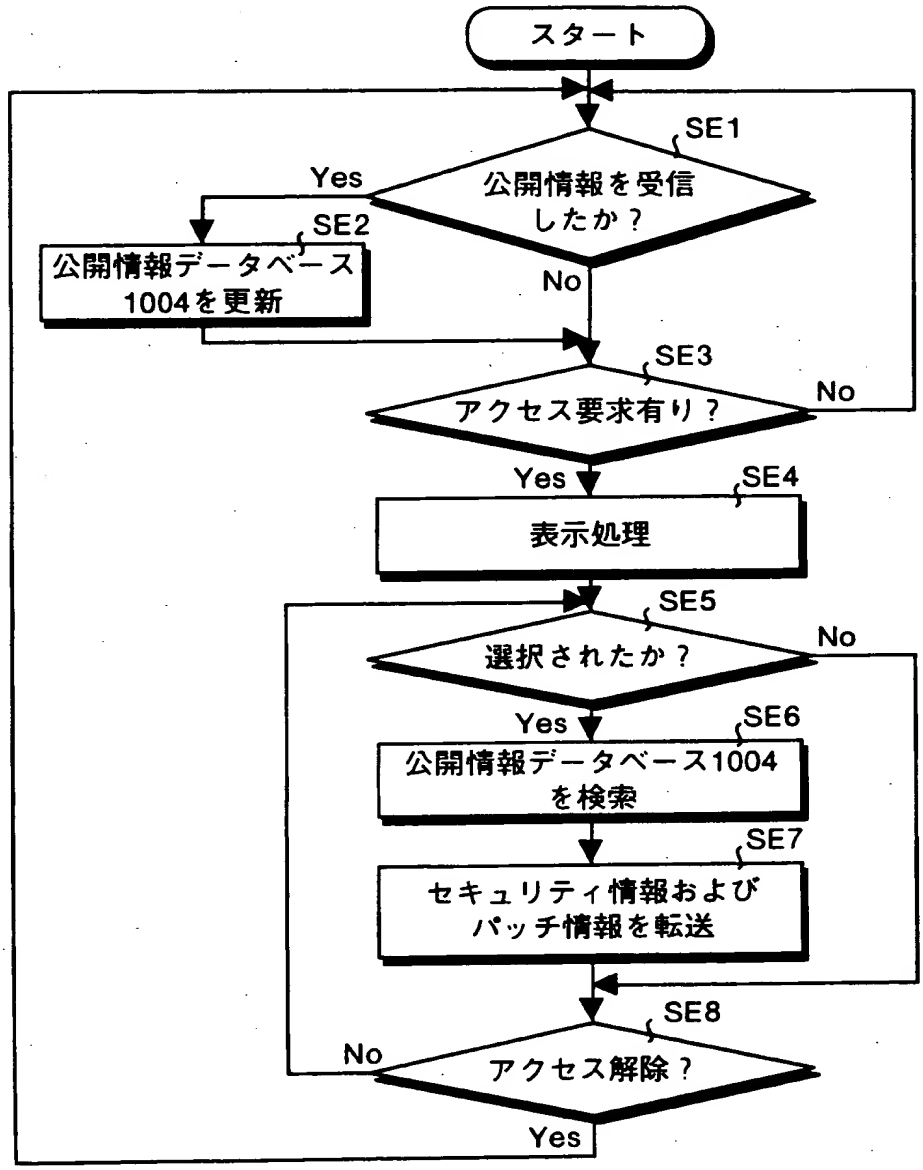
【図１５】

実施の形態４の動作を説明するフローチャート



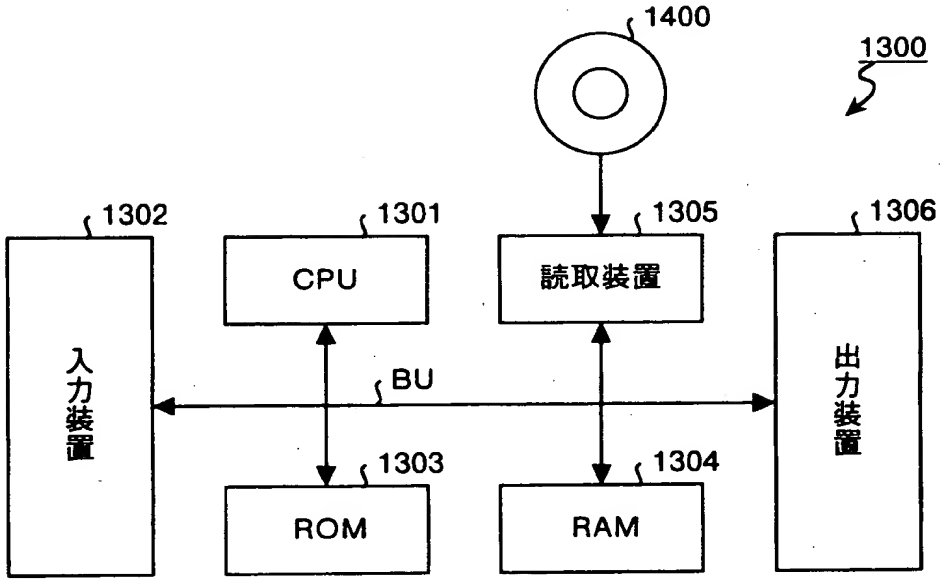
【図１６】

図12に示した情報公開部1003の動作を説明するフローチャート



【図１７】

実施の形態１～４の変形例を示すブロック図



【書類名】　　要約書

【要約】

【課題】　ユーザにとってセキュリティ情報を提供し易い環境を整備し、開発元にとって低コストで有用なセキュリティ情報を収集すること。

【解決手段】　ユーザクライアント１１から提供されたセキュリティ情報４０を登録するセキュリティ情報登録部２１と、セキュリティ情報４０の有用性を判断する開発元３１Ａの開発元クライアント３０Ａへ、セキュリティ情報登録部２１により登録されたセキュリティ情報４０を転送する転送部２３と、セキュリティ情報４０の有用性を示す返答情報４１Ａおよび当該セキュリティ情報４０の情報提供料の支払いに関する支払情報４２を開発元クライアント３０Ａより受信する返答情報登録部２４と、返答情報４１Ａおよび支払情報４２をユーザクライアント１１へ転送する転送部２６とを備えている。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社